EDITOR'S NOTE

Welcome to the third and final Issue of Volume 75 of the Federal Communications Law Journal. This year, we have had the opportunity to highlight a number of important topics within the communication law field, and this last Issue is no exception.

First, Philip Napoli and Chandlee Jackson introduce an approach to tackling disinformation and hate speech on social media that is informed by the way indecency has been regulated in the broadcast medium. Napoli is the Director of the DeWitt Wallace Center for Media & Democracy at Duke University. Jackson is a graduate of the Sanford School of Public Policy, where he earned his Masters' Degree and conducted research on the impact of disinformation on national security.

This Issue also features three student Notes. The first Note, written by Alan Harrison, discusses the right to delete, a data privacy measure that aims to give consumers greater control over their personal data. Harrison argues that, in its current form, the right to delete is too limited by exemptions and a lack of uniformity in its implementation to be fully effective.

Our second note, authored by Jamie Reiner, applies philosopher Martha Nussbaum's Capability Approach to human development to emphasize that Internet access is essential to an individual's ability to flourish. With this in mind, Reiner argues that the government has a positive obligation to promote widespread Internet access.

The third note, written by Julia Dacy, explains that the existing legal framework for protecting journalists and their confidential sources is riddled with loopholes, especially regarding the government's ability to seize communications metadata. Dacy argues that the increasing usefulness of metadata in leak investigations makes a federal shield law with specific and strong metadata provisions vital to the existence of a free press.

This issue also features our Annual Review of notable court decisions that have impacted the communications field in recent years. Each of these was authored by a member of our Journal, and we appreciate their thoughtful analyses of these important cases.

On behalf of the outgoing Editorial Board of Volume 75, I would like to thank The George Washington University Law School, our faculty advisors, and the Federal Communications Bar Association for their continued partnership. To the 2022-23 Editorial Board, Associates, Members, and authors who contributed to the Federal Communications Law Journal this year, thank you for your dedication and quality work.

Finally, congratulations to the incoming Volume 76 Editorial Board. It's been an honor to oversee this publication for its milestone 75th Volume, and I am confident the Journal is in capable hands going forward.

As always, we welcome your feedback and questions. Please send any article submissions to fcljarticles@law.gwu.edu. This issue will be archived and available at www.fclj.org.

Julia Dacy
Editor-in-Chief

Federal Communications Law Journal

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

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

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

Federal Communications Bar Association

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

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

The George Washington University Law School

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

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

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

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

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

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

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

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

FEDERAL COMMUNICATIONS LAW JOURNAL
THE TECH JOURNAL
GW LAW VOLUME 75 ISSUE 3 fcba THE TECH BAR
MAY 2023

ARTICLES

This Article considers whether there are aspects of broadcast indecency regulation that are relevant to policy deliberations about disinformation and hate speech on social media. Indecency is unique in that policymakers created a category of speech exclusive to the legal and regulatory context of a specific medium. This Article considers whether disinformation and hate speech could similarly be carved out as categories of speech that receive less First Amendment protection exclusively within the social media context. Such an approach could clear a path for modest government interventions directed at imposing greater accountability and responsibility on social media platforms.

NOTES

As States continue to pass new general privacy laws, the right to delete gains further traction. However, the right remains largely undefined with more questions than answers as to its effectiveness and implementation. This Note will focus on first clearly defining the right to delete by distinguishing it from the right to be forgotten. This step is necessary, as there is still an ongoing conflation of the two similar but distinct rights. Whereas the right to be forgotten treats the act of deletion as a mechanism to achieve the substantive goal of the digital forgetting of data (akin to human memory's natural retention limitation), the right to delete views the act of deletion as the goal itself in order to increase consumer control over one's personal data. This Note then shifts to issues in the current design of the right to delete that must be addressed to ensure the right achieves its potential within a privacy regime. The right to delete has the potential to help shift the balance of control over one's personal data, but in its current form, it will have only a limited effect. In particular, the right to delete is undermined by a lack of consistency in deletion standards and an overly broad exemption for data that is deidentified.

COMMUNICATIONS LAW: ANNUAL REVIEW

Revisiting Indecency: Considering a Medium-Specific Regulatory Approach to Disinformation and Hate Speech on Social Media

Philip M. Napoli & Chandlee A. Jackson*

TABLE OF CONTENTS

* Philip M. Napoli is the James R. Shepley Professor of Public Policy in the Sanford School of Public Policy at Duke University, where he is the Director of the DeWitt Wallace Center for Media & Democracy. Chandlee A. Jackson earned a Masters' Degree from the Sanford School of Public Policy at Duke University where he conducted research on disinformation and its impact on U.S. national security matters. This research was conducted with the support of the John S. and James L. Knight Foundation. The statements made and the views expressed are solely the responsibility of the authors.

I. INTRODUCTION

Evidence of political, psychological, medical, and cultural harms associated with social media continues to mount, particularly in light of the many revelations contained within the documents and testimony shared by Facebook whistleblower Frances Haugen.[1] In many countries, efforts to impose regulatory safeguards related to the social responsibilities of these platforms are underway.[2] In the U.S., however, we have seen relatively little consequential action at the federal level beyond ongoing antitrust inquiries, a continuing array of congressional hearings, and a series of bills that show few signs of passing.[3]

One obvious explanation for this pattern is the predominantly laissez-faire model of media regulation that has existed in the U.S., fortified by a First Amendment tradition that has erected substantial barriers to most forms of government intervention.[4] There are, of course, compelling and justifiable reasons to insulate media from regulatory intervention thoroughly laid out in long traditions of democratic theory, First Amendment jurisprudence, and legal scholarship.[5] The basic underlying premise is that the media must remain free from government interference for democracy to function effectively. The crowning irony of the current moment is that this commitment to an unregulated media sector, in which the inevitable clash between truth and falsity leads to an informed citizenry through the invisible hand of the marketplace of ideas, may evolve from its 250-year tradition of sustaining American democracy to being a driving force behind its downfall.[6]

---

1. *See* Kari Paul, *Facebook Whistleblower's Testimony Could Finally Spark Action in Congress*, GUARDIAN (Oct. 6, 2021, 5:50 PM), https://www.theguardian.com/technology/2021/oct/05/facebook-frances-haugen-whistleblower-regulation [https://perma.cc/BF7F-9H9L].

2. *See* Kim Mackrael & Rhiannon Hoyle, *Social-Media Regulations Expand Globally as Elon Musk Plans Twitter Takeover*, WALL ST. J. (May 11, 2022, 12:09 PM), https://www.wsj.com/articles/social-media-regulations-expand-globally-as-elon-musk-plans-twitter-takeover-11652285375 [https://perma.cc/W9UN-KNYQ]; *see generally* Asa Royal & Philip M. Napoli, *Platforms and the Press: Regulatory Interventions to Address an Imbalance of Power*, *in* DIGITAL PLATFORM REGULATION: GLOBAL PERSPECTIVES ON INTERNET GOVERNANCE 43 (Terry Flew & Fiona R. Martin eds., 2022).

3. *See* Meghan Anand et al., *All the Ways Congress Wants to Change Section 230*, SLATE (Mar. 23, 2021, 5:45 AM), https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html [https://perma.cc/T6QK-UGMW]; *see also* Philip M. Napoli, *The Symbolic Uses of Platforms: The Politics of Platform Governance in the United States*, 12 J. DIGIT. MEDIA POL'Y 215, 215-20 (2021); Will Oremus, *Lawmakers' Latest Idea to Fix Facebook: Regulate the Algorithm*, WASH. POST (Oct. 12, 2021, 9:00 AM), https://www.washingtonpost.com/technology/2021/10/12/congress-regulate-facebook-algorithm/ [https://perma.cc/NZY2-WTHJ].

4. For a thorough overview and discussion, see generally MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION (2019).

5. *See id.* at 15, 119.

6. *See* Tabatha Abu El-Haj, *How the Liberal First Amendment Under-Protects Democracy*, 107 MINN. L. REV. 529, 545-74 (2022); *see also* MARGARET SULLIVAN, GHOSTING THE NEWS: LOCAL JOURNALISM AND THE CRISIS OF AMERICAN DEMOCRACY 84-87 (2020); ZAC GERSHBERG & SEAN ILLING, THE PARADOX OF DEMOCRACY: FREE SPEECH, OPEN MEDIA, AND PERILOUS PERSUASION 1-3 (2022).

That being said, the prospect of government intervention remains as threatening to a well-informed citizenry and the effective functioning of the democratic process as ever[7]—perhaps more so in light of the rising political extremism in the U.S. that has emboldened political actors to attack and subvert the independence and credibility of the media sector.[8]

In this context, debates over the appropriate regulatory framework to apply to social media platforms have persisted. These deliberations have turned to the question of whether useful precedents may be found in the regulatory approaches applied to older communications technologies. For instance, there is a line of reasoning contending that the common carrier model that has traditionally applied to telephony is the appropriate fit.[9] Legislation applying this framework to social media platforms has been introduced in Congress, which would restrict platforms' ability to engage in editorial decision-making regarding the content that they carry, and instead, compel them to behave like neutral common carriers.[10] State-level legislation has passed in Texas and Florida imposing this model on social media platforms.[11] Both pieces of legislation were blocked from going into effect by the Supreme Court and the U.S. Court of Appeals for the Eleventh Circuit, respectively.[12] However, in the case of the Texas legislation, the U.S. Court of Appeals for the Fifth Circuit recently upheld the legislation's characterization of social media platforms as common carriers, concluding that "Platforms fall within the historical scope of the common carrier doctrine," which "undermines their attempt to characterize their censorship as 'speech.'"[13]

---

7. *See* Farhad Manjoo, *Regulating Online Speech Can Be a Terrible Idea*, N.Y. TIMES (May 19, 2022), https://www.nytimes.com/2022/05/19/opinion/buffalo-shooting-internet-regulations.html [https://perma.cc/72EC-SPYV].

8. *See, e.g.*, Manuel Roig-Franzia & Sarah Ellison, *A History of the Trump War on Media — The Obsession Not Even Coronavirus Could Stop*, WASH. POST (Mar. 29, 2020, 5:00 PM), https://www.washingtonpost.com/lifestyle/media/a-history-of-the-trump-war-on-media--the-obsession-not-even-coronavirus-could-stop/2020/03/28/71bb21d0-f433-11e9-8cf0-4cc99f74d127_story.html [https://perma.cc/7HUM-HQW2]; *see also The Trump Administration and the Media*, COMM. TO PROTECT JOURNALISTS (Apr. 16, 2020), https://cpj.org/reports/2020/04/trump-media-attacks-credibility-leaks/ [https://perma.cc/2RPQ-RVQQ].

9. *See* Brian Fung, *Are Social Media Platforms Like Railroads? The Future of Facebook and Twitter Could Depend on the Answer*, CNN BUS. (June 8, 2022, 10:49 AM), https://www.cnn.com/2022/06/08/tech/common-carriage-social-media/index.html [https://perma.cc/CLS5-WYYZ].

10. *See generally* 21st Century FREE Speech Act, H.R. 7613, 117th Cong. (2022).

11. *See* H.B. 20, 87th Leg., 2d Spec. Sess. (Tex. 2021) (enacted); S.B. 7072, 2021 Leg., Reg. Sess. (Fla. 2021) (enacted).

12. *See* NetChoice, LLC v. Paxton, 142 S. Ct. 1715, 1715-16 (2022) (vacating the stay of a preliminary injunction granted by the U.S. Court of Appeals for the Fifth Circuit, pending a full review of the legislation by the U.S. Court of Appeals for the Fifth Circuit); *see also* NetChoice, LLC vs. Att'y Gen., 34 F.4th 1196, 1203 (11th Cir. 2022) (finding that it is substantially likely that social media platforms are private actors whose content moderation decisions are protected by the First Amendment, but that some of the law's disclosure provisions likely do not violate the First Amendment).

13. NetChoice, LLC v. Paxton, 49 F.4th 439, 479 (5th Cir. 2022).

Another widely-embraced point of reference involves treating social media platforms like traditional publishers.[14] Doing so would involve removing the wide-ranging immunity from legal liability for content dissemination that platforms currently enjoy under Section 230 of the Communications Decency Act.[15] Traditional publishers receive no such wide-ranging immunity from liability for the content they produce.[16]

Critics have pointed out that neither component of this common carrier/publisher binary seems appropriate or satisfactory for the context at hand, and that a need for an alternative to either of these two models is required.[17] Nonetheless, there is another potentially relevant legacy media framework that has been largely ignored within current policy deliberations—broadcasting. This Article explores this third path and considers the potential applicability of applying elements of the regulatory framework developed for terrestrial broadcasting to social media platforms. This Article begins from the premise that current conditions compel us to explore whether there might be lessons from the broadcast regulatory model that are relevant to the contemporary challenges posed by the prevalence and impact of disinformation and hate speech on social media. As previous research has illustrated, there are a variety of aspects of broadcast regulation that could be relevant to how policymakers approach social media.[18]

Extending this previous work, the focal point of this analysis is that, alone amongst media technologies, broadcasting has a legally recognized and regulatable category of speech—indecency—that is exclusive to that medium. It may not be immediately clear why a discussion of broadcast indecency is relevant to contemporary concerns about disinformation and hate speech on social media. This Article's core argument is that the philosophy underlying the creation and enforcement of indecency regulations—that a particular medium may have sufficiently distinctive characteristics that justifies the creation and regulation of a category of speech exclusive to that medium—

---

14. *See* Michael Shapiro, *For Democracy's Sake, Social Media Platforms Must Be Deemed Publishers Under Section 230*, E&P (Nov. 20, 2020, 12:46 PM), https://www.editorandpublisher.com/stories/for-democracys-sake-social-media-platforms-must-be-deemed-publishers-under-section-230,180554 [https://perma.cc/XZN7-TNNQ]; *see also* Dick Lilly, *Regulate Social-Media Companies Like News Organizations*, SEATTLE TIMES (Aug. 19, 2019, 2:51 PM), https://www.seattletimes.com/opinion/regulate-social-media-companies-like-news-organizations/ [https://perma.cc/6DLT-5FR3].

15. *See* Communications Decency Act of 1996, 47 U.S.C. §§ 223, 230; *see generally* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019).

16. *See generally* Matthew Ingram, *Of Platforms, Publishers, and Responsibility*, COLUM. J. REV. (Feb. 4, 2022), https://www.cjr.org/the_media_today/of-platforms-publishers-and-responsibility.php [https://perma.cc/E38X-XEFN].

17. *See* Laura Hazard Owen, *How Can Social Media Laws Evolve Beyond the "Shoes of Newspapers or Telephones"?*, NIEMAN LAB (June 9, 2022), https://www.niemanlab.org/2022/06/can-social-media-laws-evolve-beyond-the-shoes-of-newspapers-or-telephones/ [https://perma.cc/YW3Z-6YMM].

18. *See* Philip M. Napoli, *User Data as Public Resource: Implications for Social Media Regulation*, 11 POL'Y & INTERNET 439, 439-59 (2019); *see* Philip M. Napoli, *Back from the Dead (Again): The Specter of the Fairness Doctrine and Its Lesson for Social Media Regulation*, 13 POL'Y & INTERNET 300, 300-14 (2021).

may merit consideration as an approach to dealing with social media content moderation.

The purpose of this Article, then, is to revisit the origins and rationales of the indecency standard in broadcasting and to consider what aspects of the broadcast indecency context can potentially inform current policy deliberations about whether and how to address disinformation and hate speech on digital platforms. As is increasingly clear, social media platforms are fundamentally different from broadcast media in as many ways as they are similar.[19] For this reason, there may be more utility than is commonly assumed in revisiting the history, rationales, and implementation of broadcast regulation as a point of reference for considering legal and regulatory approaches to social media platforms.

The first section of this Article provides an overview of the pattern of *technological particularism* that has characterized media law, regulation, and policy in the U.S. As this section illustrates, the legal and regulatory frameworks for media in the U.S. have been built around the notion that the nature of the regulatory requirements and First Amendment protections that apply are, to some extent, a function of the distinctive technological characteristics of each medium.[20]

The next section explores the motivations, rationales, and implementation approach of the indecency standard in terrestrial broadcasting. As this section illustrates, the indecency standard represents a singular effort by policymakers and the courts to construct and maintain a category of speech that is exclusive to a particular medium, and that comes with its own unique regulatory treatment under the First Amendment. In addressing the core rationale for the creation of the indecency category of speech, this section necessarily delves into the *pervasiveness* rationale for media regulation.[21]

The third section of this Article focuses on whether indecency provides a relevant template for approaching the problems of disinformation and hate speech on social media. This analytical focus reflects the fact that while discussions about the possibility of government intervention into the operation of social media platforms are accelerating,[22] the fundamental question regarding how such interventions could be justified in the face of First Amendment scrutiny has received relatively little attention. Thus, this section considers the parallels across broadcast indecency and social media disinformation and hate speech in terms of regulatory motivations and rationales.

---

19. *See* JOHN SAMPLES & PAUL MATZKO, KNIGHT FIRST AMEND. INST., SOCIAL MEDIA REGULATION IN THE PUBLIC INTEREST: SOME LESSONS FROM HISTORY 3-5 (2020), https://academiccommons.columbia.edu/doi/10.7916/d8-dhse-jy44/download [https://perma.cc/79DU-SEME].

20. *See, e.g.*, Jim Chen, *Conduit-Based Regulation of Speech*, 54 DUKE L.J. 1359, 1378 (2005).

21. *See* Jonathan D. Wallace, *The Specter of Pervasiveness:* Pacifica*, New Media, and Freedom of Speech* 1-3 (Cato Inst., Briefing Paper No. 35, 1998), https://www.cato.org/sites/cato.org/files/pubs/pdf/bp-035.pdf [https://perma.cc/N395-6Y54].

22. *See, e.g.*, Paul, *supra* note 1.

The concluding section summarizes the argument and considers next steps in developing this perspective into a more comprehensive policy proposal. This section also considers the question of whether the adoption of this approach is an inevitable path to government overreach and how this approach might interface with current policy proposals.

II. TECHNOLOGICAL PARTICULARISM AND U.S. MEDIA REGULATION

The term "technological particularism" has been applied in the media regulation context to describe policymakers' tendency to impose different regulatory frameworks on different communications media, with these different regulatory models derived in large part from their different technological characteristics.[23] These disparate regulatory frameworks can vary across a variety of dimensions, but perhaps most important to this analysis is the fact that these frameworks can differ in terms of the degree of First Amendment protection afforded to individual speakers.[24] As the Supreme Court noted in applying this logic to the unique regulatory framework that policymakers had constructed for broadcasting, "differences in the characteristics of new media justify differences in the First Amendment standards applied to them."[25]

This regulatory approach, with its varying degrees of First Amendment protection, has been subjected to extensive critique, with many legal scholars critical of conduit-based justifications for differing degrees of First Amendment protection.[26] As technological change (most notably, digitization) accelerated the process of convergence, in which the traditional boundaries between different media technologies and industry sectors became increasingly blurred, these critiques intensified. As Atkin noted back in 1992, specifically in reference to indecency regulation, "the fact that traditionally distinct media are now carrying each other's services—using similar modalities—calls into question the selective application of indecency in broadcasting."[27] More broadly, Levi has argued that "[i]f new technologies are indistinguishable . . . from radio and over-the-air television, then different

23. PHILIP M. NAPOLI, SOCIAL MEDIA AND THE PUBLIC INTEREST: MEDIA REGULATION IN THE DISINFORMATION AGE 143 (2019).

24. *See* Philip M. Napoli & Fabienne Graf, *Revisiting the Rationales for Media Regulation: The* Quid Pro Quo *Rationale and the Case for Aggregate Social Media User Data as Public Resource*, *in* DIGITAL AND SOCIAL MEDIA REGULATION: A COMPARATIVE PERSPECTIVE OF THE US AND EUROPE 45, 46 (Sorin Adam Matei et al. eds., 2021).

25. Red Lion Broad. Co. v. FCC, 395 U.S. 367, 387 (1969).

26. *See, e.g.*, Chen, *supra* note 20, at 1360; *see also* Frank D. LoMonte, *The "Social Media Discount" and First Amendment Exceptionalism*, 50 U. MEMPHIS L. REV. 387, 397-405 (2019).

27. David J. Atkin, *Indecency Regulation in the Wake of* Sable*: Implications for Telecommunications Policy*, 30 FREE SPEECH Y.B. 101, 103 (1992).

constitutional treatment appears arbitrary."[28] From the end-user's perspective, as convergence accelerates, traditional distinctions between media become more difficult to recognize.[29]

Despite these critiques of technological particularism, within the realm of media law and policy, "this habit has proved surprisingly durable."[30] This durability may be a function of institutional inertia.[31] In any case, this durability provides support for the exercise of exploring the social media context, which has been recognized as being fundamentally different from the Internet more broadly, across a range of factors.[32] A later section will delve more deeply into the question of whether social media might represent a compelling case for continuing a technologically particularistic approach. The next section examines one of the most pronounced manifestations of this technologically particularistic regulatory approach—the regulation of indecency in broadcasting.

III. ORIGINS, RATIONALES, AND HISTORY OF BROADCAST INDECENCY

Across the entire spectrum of U.S. media regulation, First Amendment jurisprudence, and the various categories of speech that have been identified in connection with these regulations, policies, and legal decisions, indecency is the only category of speech that has been crafted and applied specifically and exclusively within the context of a particular medium. This exclusivity is explicitly articulated in indecency's formal definition by the Federal Communications Commission ("FCC"). According to the FCC, indecency is defined as: "material that, in context, depicts or describes sexual or excretory organs or activities in terms patently offensive as measured by contemporary community standards *for the broadcast medium*."[33]

---

28. Lili Levi, *First Report: The FCC's Regulation of Indecency* 41 (U. Miami Sch. L., Rsch. Paper No. 2007-14, 2007), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1023822_code799786.pdf?abstractid=1023822&mirid=1 [https://perma.cc/QH98-783G].

29. *See* Nick Gamse, *The Indecency of Indecency: How Technology Affects the Constitutionality of Content-Based Broadcast Regulation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 287, 314 (2011).

30. Chen, *supra* note 20, at 1378.

31. It is important to note that some have argued that a regulatory approach that utilizes technology as a means of crafting individual speech environments with differing degrees of openness to government intervention represents an appropriate means of cultivating an overall speech environment that is reflective of both individual and collectivist First Amendment values. *See generally* Lee C. Bollinger, Jr., *Freedom of the Press and Public Access: Toward a Theory of Partial Regulation of the Mass Media*, 75 MICH. L. REV. 1, 1-42 (1976). For application of this argument within the more contemporary context of social media, see NAPOLI, *supra* note 23, at 144.

32. *See generally* Gerald C. Kane et al., *What's Different About Social Media Networks? A Framework and Research Agenda*, 38 MIS Q. 275, 284 (2014).

33. *Obscenity, Indecency and Profanity*, FCC, https://www.fcc.gov/general/obscenity-indecency-and-profanity [https://perma.cc/6WQY-9CL3] (last updated Dec. 20, 2022) (emphasis added).

In comparison, obscenity has no medium-specific constraints on its applicability. The Supreme Court has defined obscenity as follows:

> 1. whether the average person applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest; whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and
> 2. whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.[34]

Clearly, from a substantive standpoint, indecency represents a more restricted range of content than obscenity, with key points of distinction including the fact that indecency presumably possesses literary, artistic, political, or scientific value (whereas obscenity does not), and, of course, the fact that the indecency standard only applies in the broadcast context. Both obscenity and indecency are strongly oriented around content of a sexual nature.

Essentially, then, indecency is a category of speech that does not rise to the level of obscenity that has been crafted exclusively for application within the context of terrestrial broadcasting law, regulation, and policy.[35] This section considers how this unique category of speech came to be, as well the motivations that led to its creation.

A. Origins

The carving out of indecency as a broadcast-specific category of regulatable speech begins with the very origins of U.S. broadcast regulation—the Radio Act of 1927.[36] Included in this Act is the statement that "[n]o person within the jurisdiction of the United States shall utter any obscene, indecent, or profane language by means of radio communication."[37] This language was subsequently transferred to Section 326 of the Communications Act of 1934.[38]

Early in the history of broadcast regulation, however, neither the FCC nor the courts clearly laid out the distinction between the concepts of obscenity, indecency, and profanity, treating them instead as seemingly synonymous.[39] Efforts by policymakers or the courts to bring greater clarity to whether a meaningful distinction between these terms existed were slow to develop, due in part to the fact that, throughout much of broadcasting's early

34. *See* Miller v. California, 413 U.S. 15, 24 (1973).

35. *See* Milagros Rivera Sanchez, *The Origins of the Ban on "Obscene, Indecent, or Profane" Language of the Radio Act of 1927*, 149 JOURNALISM & MASS COMM. MONOGRAPHS 1, 10-12 (1995).

36. For a detailed history of the origins of the broadcast indecency standard, see generally *id.* This section draws heavily upon this work.

37. Radio Act of 1927, 47 U.S.C.A. § 109 (repealed 1934).

38. *See* Communications Act of 1934, 47 U.S.C. § 151.

39. *See* Rivera Sanchez, *supra* note 35, at 2-3.

history, broadcasters engaged in fairly intensive self-regulation.[40] This meant that the FCC and the courts were involved in broadcast obscenity/indecency/profanity-related issues relatively infrequently.[41]

Over time, the FCC and the courts initiated an evolutionary process in which the concept of indecency became something separate and distinct—from both a definitional and regulatory standpoint—from the concept of obscenity.[42] It was not until the mid-1960s that the FCC began to explicitly articulate that there existed a category of speech that did not rise to the level of obscenity but that still merited regulatory restriction.[43] However, at this point in time, the Commission had not yet settled on "indecent" as the preferred label.[44]

B. Toward Greater Clarity

The FCC explicitly articulated the regulatory distinction between obscenity and indecency in a 1970 decision.[45] The Commission imposed a fine upon Philadelphia radio station WUHY for an on-air interview with Grateful Dead front man Jerry Garcia, in which Garcia frequently employed a variety of profanities.[46] The Commission noted that this language did not rise to the level of obscenity but did conclude that the statutory term "indecent" should be applicable, and that in the broadcast field, the standard for its applicability should be that the material broadcast is "(a) patently offensive by contemporary community standards; and (b) is utterly without redeeming social value."[47] "The Court has made clear that different rules are appropriate for different media of expression in view of their varying natures."[48]

Here, we see the FCC lay out not only the conceptual distinction between obscenity and indecency, but also its philosophy of technological particularism—discussed above—that has undergirded the U.S. approach to media regulation.

The FCC offered further clarity in 1975, when, in a decision involving the daytime radio broadcast of George Carlin's soon-to-be-infamous Seven Words You Can Never Say on Television routine, the Commission stated that

---

40. *See id.* at 3-4.

41. *See id.* at 3.

42. For a detailed discussion of indecency and its points of distinction from obscenity, see generally Kristin A. Finch, Comment, *Lights, Camera, and* Action for Children's Television v. FCC*: The Story of Broadcast Indecency, Starring Howard Stern Comment*, 63 U. CIN. L. REV. 1275 (1994).

43. *See* Milagros Rivera Sanchez, *Developing an Indecency Standard: The Federal Communications Commission and the Regulation of Offensive Speech, 1927-1964*, 20 JOURNALISM HIST., no. 1, Spring 1994, at 9-11.

44. *Id.* at 10.

45. WUHY-FM, E. Educ. Radio, *Notice of Apparent Liability*, 24 F.C.C. 2d 408, para. 10 (1970).

46. WUHY-FM, E. Educ. Radio, *Notice of Apparent Liability*, 24 F.C.C. 2d 408, para. 16 (1970).

47. WUHY-FM, E. Educ. Radio, *Notice of Apparent Liability*, 24 F.C.C. 2d 408, para. 10 (1970).

48. *Id.*

"[t]here is authority for the proposition that the term 'indecent' . . . is *not* subsumed by the concept of obscenity—that the two terms refer to two different things."[49] The Commission went on to note that "indecent language is distinguished from obscene language in that (1) it lacks the element of appeal to the prurient interest . . . and . . . (2) when children may be in the audience, it cannot be redeemed by the claim that it has literary, artistic, political, or scientific value."[50]

The extent to which this represented new territory in the realm of media regulation is well-reflected in the fact that, as then-FCC Commissioner Glenn O. Robinson noted in his concurring statement (joined by Commissioner Benjamin Hooks), there was not, at that point in time, any "significant jurisprudence explaining the meaning" of the indecency terminology.[51] Further, then-FCC Chairman Richard Wiley explained in an interview years later that the FCC itself was not at that point clear on the difference between obscenity and indecency.[52]

It is also important to note that, at this stage, the FCC articulated that indecency was not subject to a blanket ban within the broadcast medium, but rather that it needed to be channeled to times of the day when children were not likely to be part of the audience. As the Commission stated, "[w]hen the number of children in the audience is reduced to a minimum, for example during the late evening hours, a different standard might conceivably be used."[53] Over time, and across a myriad of FCC and court decisions, as well as proposed congressional legislation, this position would ultimately evolve into the current 10:00 PM to 6:00 AM "safe harbor" for broadcast indecency that exists today.[54]

Finally, it is worth briefly noting that the FCC maintains the same regulatory framework for content deemed "profane," with profanity defined as "'grossly offensive' language that is considered a public nuisance."[55] However, given that from a regulatory standpoint, the FCC treats profanity identically to indecency (despite the different definition), and the fact that FCC and Court decisions involving profanity (offensive language of a non-sexual nature) still also (and primarily) employ the indecency terminology,[56] for simplicity's sake, the focus going forward will remain on the notion of indecency.

---

49. Citizen's Complaint Against Pacifica Found. Station WBAI (FM), *Memorandum Opinion and Order*, 56 F.C.C. 2d 94, para. 10 (1975) [hereinafter *Pacifica Found. Order*] (emphasis in original).

50. *Id.* at para. 11.

51. *Id.* at 104. (Robinson, Comm'r, concurring).

52. *See* Angela J. Campbell, Pacifica *Reconsidered: Implications for the Current Controversy over Broadcast Indecency*, 63 FED. COMM. L.J. 195, 206 (2010).

53. *Pacifica Found. Order*, 56 F.C.C. 2d at para. 12.

54. Indus. Guidance on the Comm'n's Case Law Interpreting 18 U.S.C. § 1464 & Enf't Policies Regarding Broad. Indecency, *Policy Statement*, 16 FCC Rcd 7999, para. 5 (2001).

55. *Obscene, Indecent and Profane Broadcasts*, FCC, https://www.fcc.gov/consumers/guides/obscene-indecent-and-profane-broadcasts [https://perma.cc/E6YU-8563] (last updated Jan. 13, 2021).

56. *See, e.g.*, FCC v. Fox Television Stations, Inc., 567 U.S. 239, 239 (2012).

C. The Supreme Court and Indecency

The FCC's decision in what came to be known as the "seven dirty words" case provided the basis for the Supreme Court's landmark *FCC v. Pacifica Foundation*[57] decision in 1978.[58] The Court upheld the FCC's decision, importantly noting that from a legal standpoint, the words "obscene" and "indecent" each have "a separate meaning."[59] Also important was that the Court reaffirmed the general philosophy of technological particularism, noting that "each medium of expression presents special First Amendment problems."[60] The special problems relevant to broadcasting are that "the broadcast media ha[s] established a uniquely pervasive presence in the lives of all Americans"[61] and that children were particularly vulnerable to adult content and, thus, in need of protection.

D. The Pervasiveness Rationale

It is important to note that pervasiveness is not the sole rationale for broadcast regulation. Indeed, the core rationale for broadcast regulation is that broadcasters utilize a "scarce public resource."[62] However, as demonstrated, the pervasiveness rationale is particularly central to the realm of indecency regulation.[63] Naturally, the question of whether broadcasting is now—or ever was—"*uniquely* pervasive"[64] has been the subject of much debate.[65] Clearly, the notion of broadcasting being uniquely pervasive, and this pervasiveness providing justification for different regulatory treatment, is an explicit manifestation of the technological particularism discussed earlier.

It is important to note that policymakers' efforts to expand the reach of indecency to non-broadcast technological contexts have, to this point, generally failed, due largely to the perceived lack of applicability of the pervasiveness rationale.[66] For example, the courts have overturned efforts by Congress and the FCC to regulate indecency in telephony and on cable television.[67] Within the telephony context, the Supreme Court rejected a blanket ban on obscene and indecent "dial-a-porn" services that was instituted by Congress as an amendment to the Communications Act of 1934.[68] As the Court noted in its decision, "sexual expression which is indecent but not

57. *See* FCC v. Pacifica Found., 438 U.S. 726 (1978).
58. *See* Campbell, *supra* note 52, at 201 (providing a detailed account of the arguments and deliberations that ultimately led to the *Pacifica* decision).
59. *Pacifica Found.*, 438 U.S. at 740-41.
60. *Id.* at 748 (citing Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 502-03 (1952)).
61. *Id.*
62. Napoli & Graf, *supra* note 24, at 46-47.
63. *See* Chen, *supra* note 20, at 1433.
64. FCC v. Pacifica Found., 438 U.S. 726, 727 (1978) (emphasis added).
65. *See, e.g.*, Matthew Bloom, *Pervasive New Media: Indecency Regulation and the End of the Distinction Between Broadcast Technology and Subscription-Based Media*, 9 YALE J.L. & TECH. 109, 115, 118 (2006); Wallace, *supra* note 21, at 10.
66. *See* Wallace, *supra* note 21, at 5.
67. *See* Atkin, *supra* note 27, at 105-08.
68. Sable Comm. of Cal., Inc. v. FCC, 492 U.S. 115, 131 (1989).

obscene is protected by the First Amendment."[69] Further, the Court noted that *Pacifica* was not applicable, given that dial-up services require users to "take affirmative steps to receive the communication."[70] According to the Court:

> There is no "captive audience" problem here; callers will generally not be unwilling listeners. The context of dial-in services, where a caller seeks and is willing to pay for the communication, is manifestly different from a situation in which a listener does not want the received message. Placing a telephone call is not the same as turning on a radio and being taken by surprise by an indecent message. Unlike an unexpected outburst on a radio broadcast, the message received by one who places a call to a dial-a-porn service is not so invasive or surprising that it prevents an unwilling listener from avoiding exposure to it.[71]

In the cable television context, the Supreme Court struck down a provision in the Telecommunications Act of 1996 which required cable television providers to completely scramble or block channels that are primarily dedicated to sexually-oriented programming or limit their transmission to the hours of 10:00 PM to 6:00 AM (akin to the channeling parameters established for broadcast indecency).[72] As with *Sable,* the fact that the policy extended into the realm of indecent speech was a factor in the Court's decision.[73] As Justice Clarence Thomas noted in his concurring opinion,

> What remains then is the assumption that the programming restricted by § 505 is not obscene, but merely indecent. The Government, having declined to defend the statute as a regulation of obscenity, now asks us to dilute our stringent First Amendment standards to uphold § 505 as a proper regulation of protected (rather than unprotected) speech.[74]

Once again, the Court based its decision on fundamental differences between media. In noting the inapplicability of *Pacifica,* the Court noted that, "[t]here is, moreover, a key difference between cable television and the broadcasting media, which is the point on which this case turns: Cable systems have the capacity to block unwanted channels on a household-by-household basis."[75]

---

69. *Id.* at 126.
70. *Id.* at 128.
71. *Id.*
72. *See* United States v. Playboy Ent. Grp., Inc., 529 U.S. 803, 806, 827 (2000).
73. *See id.* at 814 ("[E]ven where speech is indecent and enters the home, the objective of shielding children does not suffice to support a blanket ban if the protection can be accomplished by a less restrictive alternative.").
74. *Id.* at 830.
75. *Id.* at 815.

In addition, efforts by Congress to bring indecency regulation to the Internet in the form of the Communications Decency Act of 1996[76] were similarly rejected,[77] with the Supreme Court noting that, "the Internet is not as 'invasive' as radio or television," requiring more "affirmative steps" on the part of users.[78] Ultimately, the constitutionality of indecency regulation seems to hinge on the distinction between "push" and "pull" media; that is between "media that deliver information passively and those that await user intervention."[79] A push medium, it would seem, is inherently more pervasive.

IV. EXTENDING THE BROADCAST INDECENCY LOGIC: DISINFORMATION, HATE SPEECH, AND SOCIAL MEDIA

The goal thus far has been to illustrate the motivations and rationales of the broadcast indecency standard and to illustrate how they have, to this point, been found by the Supreme Court to not be transferrable to other media. As has been made clear, indecency is a broadcast-specific category of speech. The creation and maintenance of the indecency standard has been motivated primarily (though not exclusively) by the need to protect a particularly vulnerable group (children). And, importantly, the application of the indecency standard has been limited to a medium possessing certain distinguishing characteristics, notably a unique pervasiveness but also one that utilizes a scarce public resource. This section considers whether the general underlying principles that have led to the creation and continued application of the indecency standard in broadcasting might be transferable to completely different speech contexts (disinformation and hate speech) on a completely different medium (social media).

Indeed, the goal of this section is not to argue for—or even consider—the wholesale transference of the indecency standard to the social media platform context (in a manner similar to what Congress attempted with the Internet and the Communications Decency Act of 1996).[80] Rather, the goal of this section is to consider whether the fundamental notion of crafting a distinctive category of speech that, from a regulatory standpoint, is exclusive to a specific medium, might be a viable path forward in the context of social media platform regulation. Specifically, this section considers the possibility of categorizing disinformation and hate speech as distinctive categories of speech that, within the narrow context of large social media platforms such as Facebook, Twitter, Tik Tok, and YouTube, are subject to a lower level of First Amendment protection and, thus, more intensive government regulation. These categories of speech would remain constitutionally protected in other

76. Communications Decency Act of 1996, 47 U.S.C. §§ 223, 230.

77. Maria Fontenot & Michael T. Martínez, *FCC's Indecency Regulation: A Comparative Analysis of Broadcast and Online Media*, 26 UCLA ENT. L. REV. 59, 67 (2019).

78. Reno v. ACLU, 521 U.S. 844, 853-70 (1997).

79. Chen, *supra* note 20, at 1433-34.

80. Telecommunications Act of 1996, 47 U.S.C. § 223(a)(I)(B)(ii), 223(d) (1994 ed., Supp. II). (These sections of the Telecommunications Act of 1996 were subsequently struck down by the Supreme Court in *Reno v. ACLU*). *See* Reno, 521 U.S. at 853-70.

communicative contexts, given the First Amendment's established wide-ranging protections for falsity and hate speech.[81]

This section begins by acknowledging that disinformation and hate speech are far from exclusively social media problems. Traditional media forms, such as print, cable television (e.g., certain cable news networks), and broadcast radio (in particular political talk radio), are also substantial contributors.[82] Indeed, a growing sphere of critique argues that the academic community's and popular press' fixation on disinformation on social media has exaggerated social media's overall contribution, and perhaps more important, has distracted attention away from understanding and addressing the broader underlying causes of, and defenses against, disinformation.[83]

Nonetheless, the unprecedented scale of social media platforms' operations (in terms of both audience reach and content distributed) has meant that they have been well-documented contributors to the broader disinformation and hate speech problem.[84] Given that at this point—at least in the U.S.—these platforms operate free of any regulatory obligations to police disinformation and hate speech, exploration of possible mechanisms for altering the status quo seem warranted. The framework for this analysis involves considering which aspects of the broadcast indecency model translate to the social media disinformation/hate speech context and which do not.

A. Motivations

Examining motivations is an appropriate starting point. Within the broadcast context, the primary (though not exclusive) motivation for indecency regulation has been the protection of children from harmful content. This is the "compelling government interest" that is essential for any government intrusions into speakers' First Amendment rights.[85]

---

81. For overviews of the First Amendment protections afforded disinformation and hate speech, see generally G. Edward White, *Falsity and the First Amendment*, 72 SMU L. REV. 513 (2019), and Lauren E. Beausoleil, *Free, Hateful, and Posted: Rethinking First Amendment Protection of Hate Speech in a Social Media World*, 60 B.C. L. REV. 2101 (2019).

82. Emily Bazelon, *The Problem of Free Speech in an Age of Disinformation*, N.Y. TIMES MAG. (Oct. 13, 2020), https://www.nytimes.com/2020/10/13/magazine/free-speech.html [https://perma.cc/G7VW-6DGT].

83. *See* Joseph Bernstein, *Bad News: Selling the Story of Disinformation*, HARPER'S MAG., Sept. 2021, at 25, 31.

84. *See generally* NAPOLI, *supra* note 23; YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS (2018); Caroline Atkinson et al., *Recommendations to the Biden Administration on Regulating Disinformation and Other Harmful Content on Social Media* 4 (Harvard Kennedy Sch., Mossavar-Rahmani Ctr. for Bus. & Gov't, Working Paper No. 2021-02, 2021), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/FWP_2021-02.pdf [https://perma.cc/8QWN-UPEJ]; ANDREA C. NAKAYA, SOCIAL MEDIA HATE SPEECH: THE RISKS OF SOCIAL MEDIA (2020).

85. *See, e.g.*, Ronald Steiner, *Compelling State Interest*, FIRST AMEND. ENCYC., https://www.mtsu.edu/first-amendment/article/31/compelling-state-interest [https://perma.cc/GG25-SQWG] (last visited Mar. 13, 2023).

As has been noted, a key motivator for broadcast indecency regulations has been the protection of children from harmful content. Many of the revelations from Facebook whistleblower Frances Haugen focused on harms suffered by children, in relation to issues such as bullying, body image problems, and addiction.[86] Thus, the motivation for protecting children would persist here and easily extend to disinformation and hate speech. Just as children are more vulnerable than adults to the negative effects of exposure to indecent programming, it would stand to reason that they are also more vulnerable to the negative effects of exposure to disinformation and hate speech.[87]

One could even go further and argue that, within the contexts of disinformation and hate speech, there are other groups that are similarly vulnerable and in need of protection. Consider, for instance, the growing body of research indicating that the elderly are particularly susceptible to accepting disinformation that they encounter on social media as truth and to sharing it with others. Research has found that elderly social media users are significantly over-represented amongst "supersharers"—a group responsible for over eighty percent of fake news sharing on social media.[88] On Facebook, compared to young users, those over sixty-five shared seven times more links to fake news domains.[89] The effect of age was found to hold after controlling for other explanatory factors, such as partisanship, education, and overall posting activity.[90]

Such findings are particularly concerning because voters over sixty-five have the highest rate of voter turnout of any age category.[91] Essentially, then, a group with the greatest engagement with the democratic process is most susceptible to organized efforts to subvert this process—a process that presumably there is a compelling state interest in protecting.

There are a number of possible explanations for this pattern. Researchers have highlighted factors such as less online experience,

---

86. *See generally,* Paul, *supra* note 1; Dan Milmo & Kari Paul, *Facebook Harms Children and Is Damaging Democracy, Claims Whistleblower*, GUARDIAN (Oct. 6, 2021), https://www.theguardian.com/technology/2021/oct/05/facebook-harms-children-damaging-democracy-claims-whistleblower [https://perma.cc/ZF43-9ZG7].

87. *See generally* PHILIP N. HOWARD ET AL., UNICEF OFF. OF GLOB. INSIGHT & POL'Y, DIGITAL MISINFORMATION / DISINFORMATION AND CHILDREN (2021), https://www.ictworks.org/wp-content/uploads/2021/10/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf [https://perma.cc/YY7G-PBE88]; Julia Kansok-Dusche et al., *A Systematic Review on Hate Speech Among Children and Adolescents: Definitions, Prevalence, and Overlap with Related Phenomena*, 25 TRAUMA, VIOLENCE, & ABUSE (forthcoming 2024) (manuscript available at https://journals.sagepub.com/doi/pdf/10.1177/15248380221108070 [https://perma.cc/G5TR-AT4W]).

88. Nir Grinberg et al., *Fake News on Twitter During the 2016 Presidential Election,* 363 SCIENCE 374, 375 (2019).

89. Andrew Guess et al., *Less than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook,* 5 SCI. ADVANCES 2 (2019).

90. *Id*.

91. Press Release, U.S. Census Bureau, 2020 Presidential Election Voting and Registration Tables Now Available (Apr. 29, 2021), https://www.census.gov/newsroom/press-releases/2021/2020-presidential-election-voting-and-registration-tables-now-available.html [https://perma.cc/DNU4-C3VX].

suboptimal capacity for judgment, and higher levels of trust in one's social network.[92] These are descriptors that, needless to say, could just as easily be applied to children. However, the key difference here is that children do not vote (though certainly a child reared on disinformation is not likely to grow into a well-informed participant in the democratic process).

The inherent vulnerability of the elderly to other forms of disinformation, such as online and telephone scams, has been recognized by policymakers,[93] and has led to the enactment of speech-related laws and regulations that are explicitly motivated by the need to protect this sector of the population.[94] The 2018 Senior Safe Act, for instance, allows banks, credit unions, investment advisers, and brokers to report suspected fraud against seniors to law enforcement without fear of being sued, as long as they have trained their employees in how to detect suspicious activity.[95] In a recent request that the FCC take more aggressive enforcement actions implementing existing regulations regarding robocalls, Senators Edward Markey and John Thune noted:

> Although Congress, the FCC, private companies, and consumer advocates have taken important steps to address the plague of robocalls in recent years, Americans continue to receive illegal robocalls. In many cases, these calls inflict serious harm on consumers and can lead to significant financial damage to members of vulnerable communities, particularly more elderly individuals.[96]

Vulnerable communities are central to concerns about the proliferation of hate speech on social media platforms as well. Obviously, the subjects of hate speech face the risks of violence, social marginalization, and the accompanying psychological effects that can arise from hate speech. Targets of social media-disseminated hate speech tend to be populations with a

---

92. *See* Nadia M. Brashier & Daniel L. Schacter, *Aging in an Era of Fake News*, 29 CURRENT DIRECTIONS PSYCH. SCI. 316, 317-19 (2020).

93. *See* Lilianne Daniel et al., *Protecting the Public and Vulnerable Populations from Fraudulent Scams on Social Media*, NAT'L ASS'N OF ATT'YS GEN. (Apr. 12, 2019), https://www.naag.org/attorney-general-journal/protecting-the-public-and-vulnerable-groups-from-fraudulent-scams-on-social-media/ [https://perma.cc/ZPC3-5BC8]; *see also* FED. BUREAU OF INVESTIGATION, 2021 IC3 ELDER FRAUD REPORT 3 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf [https://perma.cc/W9BV-5KTK].

94. *See* Slide Deck Presentation, Odette Williamson, Att'y, Nat'l Consumer L. Ctr., & Lisa Weintraub Schifferle, Att'y, Fed. Trade Comm., Nat'l Ctr. on L. & Elder Rts., Legal Basics: Protecting Older Adults Against Scams, at slide no. 5 (Apr. 10, 2018), https://ncler.acl.gov/pdf/Protecting%20Older%20Adults%20Against%20Scams%20Slides.pdf [https://perma.cc/GW7W-N6HB].

95. *See* Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub L. No. 115-174, § 303, 132 Stat. 1296, 1335-38 (2018) (Senior Safe Act).

96. Letter from Edward J. Markey & John Thune, U.S. Senators, to The Hon. Jessica Rosenworcel, Chairwomen, FCC 1 (Feb. 3, 2022) (available at https://www.markey.senate.gov/imo/media/doc/letter_-_fcc_itg.pdf [https://perma.cc/4Y9P-TCZB]).

minority status, with hate speech essentially compounding their vulnerabilities.[97] Researchers have documented effects on hate speech victims:

> [They have e]xperienced physiological and emotional symptoms ranging from rapid pulse rate and difficulty in breathing, to nightmares, post-traumatic stress disorder, psychosis and suicide. [Attacks have resulted in] deep emotional scarring, and feelings of anxiety and fear that pervade every aspect of a [hate speech] victim's life.[98]

It is important to emphasize that in both the disinformation and hate speech contexts, there is a growing body of evidence that—particularly on social media—traditional remedies to "bad speech," such as counterspeech, are ineffective.[99] For instance, a study of hate speech on Twitter found that counterspeech from a white speaker could discourage racist hate speech; but if that same counterspeech originated from a Black speaker, the amount of hate speech was not affected at all.[100] Such findings suggest that targets of hate speech may be uniquely powerless to utilize counterspeech.

In the disinformation context, research has identified a wide range of factors that explain why, particularly in the social media context, disinformation can easily be over-produced relative to factual news and information, why it tends to travel faster through social networks than factual news information, and why individuals are likely to not be exposed to—or not respond favorably to—factual corrections to disinformation.[101] Such findings further undermine the traditional reliance on counterspeech as a remedy.

The key point here is that, as is the case with indecency, there are specific communities that have proven to be uniquely vulnerable to the effects of disinformation and hate speech on social media. That being said, there is no reason to assume that the identification of a vulnerable group is fundamental to the carving out of a less-protected category of speech. No FCC or court decision has articulated such a principle of exclusivity. Presumably, such an action could also be motivated by other compelling government interests, such as the preservation of the democratic process, which the First

---

97. The United Nations ("UN") published investigative findings on hate speech on social media which contextualized the experiences of populations uniquely vulnerable to hate speech. *See Targets of Hate*, U.N.: HATE SPEECH, https://www.un.org/en/hate-speech/impact-and-prevention/targets-of-hate [https://perma.cc/5SN2-T56A] (last visited July 21, 2022). The UN calculated that 70 percent or more of the targets of hate speech internationally are populations belonging to a minority status, specifically national, ethnic, religious, or linguistic minorities. *Id.*

98. Michael J. Cole, *A Perfect Storm: Race, Ethnicity, Hate Speech, Libel and First Amendment Jurisprudence*, 73 S.C. L. REV. 437, 444 (2021).

99. For an overview of this evidence, see generally Philip M. Napoli, *What if More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMM. L.J. 55 (2018).

100. *See* Kevin Munger, *Tweetment Effects on the Tweeted: Experimentally Reducing Racist Harassment*, 39 POL. BEHAV. 629, 642 (2017).

101. For a detailed discussion of these findings, see Napoli, *supra* note 98, at 68.

Amendment is intended to support in part through the cultivation of an informed citizenry.[102] Disinformation undermines the well-informed decision making that is central to a well-functioning democracy, potentially leading to a form of market failure in the marketplace of ideas.[103]

B. Rationales

Within the U.S. approach to media regulation, compelling motivations typically are not sufficient for government intervention. There must also be a compelling rationale—characteristics of the particular mediated context that provide justifications to pursue the motivation in question.[104] As was noted previously, indecency regulations were premised in large part on the rationale that the broadcast medium was uniquely pervasive, widely and freely available, and virtually universally adopted and used. As noted above, the application (or lack thereof) of indecency regulations to other media hinged, in large part, on whether these media were similarly pervasive. From the Court's perspective, the answer to this question has consistently been no.[105]

It should be noted that the regulation of broadcast content (particularly in relation to news and information, which is the focus here) has been premised on rationales other than pervasiveness, such as broadcasters' use of a scarce public resource.[106] Consequently, a compelling case can be made that if one of these other rationales were found to apply, then that might be sufficient to justify some form of disinformation regulation for social media platforms.[107] This is a topic that is beyond the scope of this analysis but has been dealt with extensively elsewhere.[108]

Here, we take up the question of whether there is a compelling case to be made that contemporary social media platforms possess the kind of pervasiveness that characterized broadcasting at the peak of its reach and influence.[109] Toward this end, it would certainly be useful if either the FCC or the courts had fleshed out the notion of pervasiveness in substantial detail. Unfortunately, this is not the case. We are, however, left with a few basic components upon which we can build this analysis.

---

102. *See* PHILIP M. NAPOLI, FOUNDATIONS OF COMMUNICATIONS POLICY: PRINCIPLES AND PROCESS IN THE REGULATION OF ELECTRONIC MEDIA 37 (2001).

103. *See* Napoli, *supra* note 99, at 97-98.

104. *See* NAPOLI, *supra* note 23, at 144-48.

105. *See supra* pp. 307-08.

106. *See, e.g.*, Napoli & Graf, *supra* note 24, at 47.

107. *See* Philip M. Napoli & Fabienne Graf, *Social Media Platforms as Public Trustees: An Approach to the Disinformation Problem*, *in* ARTIFICIAL INTELLIGENCE AND THE MEDIA: RECONSIDERING RIGHTS AND RESPONSIBILITIES 93, 107-15 (Taina Pihlajarinne & Anette Alén-Savikko eds., 2022).

108. Napoli, *supra* note 18, at 442; Philip M. Napoli, *Treating Dominant Digital Platforms as Public Trustees*, *in* REGULATING BIG TECH: POLICY RESPONSES TO DIGITAL DOMINANCE 151, 145-47 (Martin Moore & Damian Tambini eds., 2021).

109. For a pre-social media effort to conduct a similar analysis in relation to post-broadcast technologies, such as cable, satellite, and Internet radio, see Bloom, *supra* note 65, at 117-26.

At the most basic level, there is the issue of reach. As the Supreme Court noted in *Pacifica*, a key aspect of what made broadcasting pervasive was its "presence in the lives of all Americans."[110] This statement reflects the near universality of broadcasting's reach and influence circa 1978. Of course, no one broadcaster had this kind of reach, due to the license allocation system that granted licenses at the local level and due to broadcast station ownership limits (much more stringent than now) that limited the national reach of any one owner.[111] But the medium itself was essentially ubiquitous, with the traditional Big Three broadcast networks accumulating massive audiences through their networks of local affiliates.[112] The same degree of ubiquity can be found for social media today, with social media usage exceeding eighty-two percent in 2021 and still trending upward.[113] And today, individual platforms, such as Facebook and YouTube, are used by a substantial proportion of the American public [114] in a way that is comparable to how the public relied upon the Big Three broadcast networks at their peak. These networks each reached ninety-seven percent of American households and divided that audience amongst themselves with relatively little competition.[115] Thus, from the reach dimension of pervasiveness, social media—both collectively and in terms of individual networks—would seem to meet or exceed broadcasting.

Another distinguishing characteristic that is, to some degree, implicit in the notion of pervasiveness is the distinction between media available for free and media requiring audience payment.[116] This distinction is part of the reason why the FCC and the courts have refused to characterize media such as cable television and satellite radio as pervasive, even though from an end user's standpoint, they are virtually identical to their free, ad-supported counterparts, broadcast television and radio.[117] When consumer payment/subscription is involved, not only can this payment/subscription arrangement be interpreted as a more affirmative step on the part of the end user to receive the content, it can also facilitate mediation of the relationship between content provider and

110. FCC v. Pacifica Found., 438 U.S. 726, 748 (1978).

111. For an overview of the current state of U.S. media ownership regulations and of how they have evolved over time, see generally DANA A. SCHERER, CONG. RSCH. SERV., R43936, THE FCC'S RULES AND POLICIES REGARDING MEDIA OWNERSHIP, ATTRIBUTION, AND OWNERSHIP DIVERSITY (2016).

112. *See id.* at 20-21.

113. *See* Slide Deck Presentation, Edison Rsch. & Triton Digit., The Infinite Dial 2021, at slide no. 20 (Mar. 11, 2021), http://www.edisonresearch.com/wp-content/uploads/2021/03/The-Infinite-Dial-2021.pdf [https://perma.cc/6R5M-SLCW]. The Infinite Dial is the longest-running survey of digital media consumer behavior. *Id.* at slide no. 2.

114. *See Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/6264-RKBF].

115. For an overview of the era of Big Three network dominance, see generally KEN AULETTA, THREE BLIND MICE: HOW THE TV NETWORKS LOST THEIR WAY (1992).

116. *See* Bloom, *supra* note 65, at 122.

117. *Id.*

end user on an individual level,[118] unlike the more indiscriminate nature of the relationship between broadcasters and their audiences.

A third articulated dimension of pervasiveness (related to the free component) has been the likelihood of accidental exposure to harmful or offensive content. In the broadcast context, this meant that one could be listening or watching some free, widely available broadcast programming, and unexpectedly and involuntarily be exposed to indecent programming. As the Supreme Court noted in the *Pacifica* case, "prior warnings cannot completely protect the listener or viewer from unexpected program content."[119]

Comparable situations arise in the social media disinformation/hate speech context when we consider users scrolling through their news feeds from a freely available social media platform and suddenly being exposed to posts containing anything from the livestream of a shooting to racist hate speech, to, of course, various categories of disinformation. And while social media users make affirmative decisions about which other accounts to follow, the operation of many contemporary social media platforms is such that a user's news feed is increasingly populated by content from other accounts that the platforms' curation algorithms have determined the user is likely to find interesting.[120] This is, in many ways, the central problem with social media—the extent to which individual users are now saddled with the challenge of processing and making sense of the disparate stream of content that social media platforms push at them.

This brings us to the important distinction noted earlier between "push" and "pull" media. As has been argued elsewhere, the fundamental transformation that social media imposed on the Internet was the shift from a pull medium to a push medium.[121] While the notion of the traditional Web being pervasive can be countered by the 1990s-2000s-era Internet user's need to proactively seek out content, by the 2010s, social media flipped that dynamic, pushing streams of content to users without them having to take the traditional proactive steps. And so, to the extent that the notion of pervasiveness depends at least in part on whether a medium has a "push" orientation, social media platforms possess that fundamental characteristic, whereas the broader Internet largely does not.

In sum, though it is questionable whether the core dimensions of the pervasiveness rationale need to be met in order to borrow the medium-specific speech carve-out model from broadcast regulation, the analysis presented in this section suggests that the basic criteria that policymakers and the courts have applied to broadcasting in order to characterize the medium as pervasive—and to bolster their justification for indecency regulation—seem to translate reasonably well to the social media context.

---

118. *See* United States v. Playboy Ent. Grp., Inc., 529 US 803, 804 (2000).

119. FCC v. Pacifica Found., 438 U.S. 726, 748 (1978).

120. Michael Kan, *Facebook, Instagram to Show You More Content from People You Don't Follow*, PC MAG. (July 28, 2022), https://www.pcmag.com/news/facebook-instagram-to-show-you-more-content-from-people-you-dont-follow [https://perma.cc/LS89-AQ2A].

121. NAPOLI, *supra* note 23, at 42-48.

As was noted above, the notion of pervasiveness as a regulatory rationale remains woefully under-developed, heightening its vulnerability to critique. Nonetheless, the pervasiveness rationale and its associated regulatory carve-out for broadcast indecency remain accepted precedent in U.S. media law and policy, maligned as they may be from many quarters. As policymakers today consider possible approaches to address the problem of disinformation and hate speech on social media, considering these as regulatable categories of speech exclusively within the context of social media, while continuing to remain free to circulate on the broader Internet and other mediated contexts, may be an idea worthy of further consideration.

V. CONCLUSION

The proposal put forth here is, in many ways extreme, particularly in light of the way in which the dominant media regulatory philosophy has evolved since the days when regulatory obligations, such as indecency and the Fairness Doctrine, were being introduced and fleshed out.[122] These regulatory requirements represent the apex of government intervention into the media sector and have, retrospectively, been characterized by many critics as the epitome of government overreach.[123] The question implicit in this analysis is whether we might be at another moment when a deviation from the more established philosophical norm might be in order. If the answer to that question is yes, then this Article has laid out a foundation for charting a path forward.

Obviously, this Article has focused on the core issues of motivations and rationales upon which any media regulatory framework is built. It has not tackled the complex definitional and implementation challenges that would, of course, be essential next steps. As the history of concepts such as obscenity and indecency has taught us, defining such terms is inherently fraught, and the end result is likely to be imperfect. But the task is not impossible. In its re-examination of indecency regulation, this Article has identified some potential starting points from an implementation standpoint. For instance, what is the social media equivalent of "channeling" disinformation/hate speech in a way that is analogous to how broadcasters have been required to channel indecency to the late-night hours? Is the process of algorithmic amplification the appropriate analogue? If it is, could we imagine a regulatory framework that requires that platforms refrain from algorithmically amplifying posts that the platforms' own processes determine to be disinformation or hate speech? Could we imagine an approach akin to indecency's focus on a particularly vulnerable population but focused on channeling the harmful content away from audience segments that have a similarly empirically demonstrated vulnerability?

Finally, a key caveat of this analysis: embracing that social media may represent a unique context where disinformation and/or hate speech may be

122. For discussions of this evolution in regulatory philosophy, see generally Napoli (2021), *supra* note 18, at 304-05; SCHERER, *supra* note 111.

123. *See, e.g.*, Napoli (2021), *supra* note 18, at 306.

subject to less First Amendment protection does not automatically create an authoritarian model of media regulation any more than treating broadcasters as trustees of a scarce public resource has. Broadcasters have maintained a substantial degree of First Amendment protection. And so, when we think of the implications of this analysis for future social media regulation, it would be a mistake to jump to extreme conclusions about some form of an authoritarian Ministry of Truth, passing self-interested judgment on the veracity of individual social media posts.

Indeed, it is important to keep in mind that some of the even fairly modest regulatory proposals that have been put forth by various stakeholders—such as requiring social media platforms to develop their own standards of conduct related to the policing of disinformation and hate speech; mandating increased accountability for the behaviors of disinformation super spreaders; or scaling back the expansive Section 230 liability protections exclusively in relation to disinformation, or to algorithmically amplified content more broadly[124]—would likely incur First Amendment challenges. The analysis presented here suggests that there may exist an established means of overcoming such challenges based on precedents developed within the context of indecency in broadcasting.

124. *See, e.g.*, ASPEN DIGIT., COMMISSION ON INFORMATION DISORDER FINAL REPORT 5 (2021), https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf [https://perma.cc/7UK8-9WBH]; Atkinson et al., *supra* note 84, at 7.

Where Next for the Right to Delete: Stepping Out of the Shadow of the Right to be Forgotten

Alan Harrison*

TABLE OF CONTENTS

* J.D., May 2023, National Security and Cybersecurity Concentration, The George Washington University Law School, and Research Assistant for Professors Daniel J. Solove, John Marshall Harlan Research Professor of Law, and Laura A. Dickinson, Oswald Symister Colclough Research Professor of Law. M.P.S., May 2019, Legislative Affairs, Graduate School of Political Management, George Washington University. B.A., May 2016, Economics and Political Science, George Washington University. I have immense gratitude towards the staff and Editorial Board members of the FCLJ for their publication support and comments, and to all those who supported this note's development, including: Meredith Rose and Natasha Nerenberg, my Journal Adjunct Advisor and Notes editor; Professor Solove; Stacey Gray and Amie Stepanovich, Senior Director for U.S Policy and Vice President for U.S. Policy at the Future of Privacy Forum for their early encouragement of this topic; and lastly to my family for all of their encouragement.

I. INTRODUCTION

In 2018, California enacted the California Consumer Privacy Act ("CCPA"), granting California consumers a number of rights against data-holders to give them "more control over [their] personal data."[1] One of these rights is the right to request that a business or organization delete one's personal information.[2] Concerns linger regarding how to implement the statute's right to delete ("RTD"); of particular concern are the numerous exceptions to the right.[3] Other states have enacted their own state privacy statutes with Virginia, Colorado, and Utah all including the RTD with similar exemptions within their state privacy bills.[4]

While the RTD has been gaining traction in current and pending privacy bills in the United States, there has been little focus on its scope, effect, and technical implementation. This Note delves into the RTD with the intent of analyzing its immediate limitations that prevent the right from realizing its full effectiveness within a consumer privacy regime of rights.

The first step in analyzing the RTD in its current form is to clearly define the right. Imbedded with that step, however, is an antecedent step of distinguishing the RTD from the right to be forgotten ("RTBF"). The RTD (which is the European functional equivalent to the right of "erasure") is often

1. *California Consumer Privacy Act (CCPA)*, OFF. OF ATT'Y GEN., STATE OF CA. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/ccpa [https://perma.cc/6M5T-CY6Q] (last visited Mar. 27, 2022).

2. *Id.*

3. Yoni Bard & Scott Bloomberg, *CCPA: The (Qualified) Right to Deletion*, JD SUPRA (July 25, 2019), https://www.jdsupra.com/legalnews/ccpa-the-qualified-right-to-deletion-40847 [https://perma.cc/37UQ-MV88]; *see also* Ilia Sotnikov, *Six Top Concerns of CCPA Compliance*, SECURITYINFOWATCH.COM (Apr. 29, 2019), https://www.securityinfowatch.com/cybersecurity/information-security/article/21078368/six-top-concerns-of-ccpa-compliance [https://perma.cc/L45U-SLH9] (describing numerous first-glance issues of the CCPA as proposed, including a "list of exceptions [to the right to delete] so broad that companies can come up with legitimate excuses not to delete data at all.").

4. *See* Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-571-581 (West, 2022), Colorado Privacy Act, COLO. REV. STAT. ANN. §§ 6.1.1301-1313 (West, 2023), S.B. 1392, 161st Gen. Assemb., 1st Spec. Sess. (Va. 2021) (enacted, Consumer Data Protection Act); S.B. 21-190, 73rd Gen. Assemb., Reg. Sess. (Colo. 2021) (enacted, Colorado Privacy Act); S.B. 227, 2022 Leg., Gen. Sess. (Utah 2022) (enacted, Utah Consumer Privacy Act); Jake Holland, *Utah Privacy Bill Signed, Making Fourth State with Such a Law*, BLOOMBERG LAW (Mar. 24, 2022, 2:56 PM) https://news.bloomberglaw.com/privacy-and-data-security/utah-privacy-bill-signed-marking-fourth-state-with-such-a-law [https://perma.cc/BY3X-SJR6].

either conflated with the RTBF or analyzed in relation to the RTBF.[5] While they share similar characteristics, in part because of the technical nature of implementing each right, they are clearly distinct rights with different purposes.

The second step for this Note—once the RTD has been clearly distinguished from the RTBF—is to address the most critical issues that will help ensure the effectiveness and full scope of the RTD. The most significant issue is the lack of standardization in the definition and the technical process of "deletion" once a consumer submits a request to an entity to delete their personal data. This lack of consistency stems from the variety of state data disposal laws (which will control in each state that passes a state privacy law) and the absence of a standard definition of deletion within privacy bills that aligns with technical definitions of deletion. Almost as critical is the issue of exemptions to consumer requests to delete personal data when an entity deidentifies (or pseudonymizes) personal data in lieu of deletion. This Note suggests that this exemption grants a false sense of security to the consumer and potentially defeats the purpose of the RTD due to recent leaps forward in reidentification science. Thus, consumer deletion requests that are exempted in this way defeat the purpose of the right, which is to shift the balance of control over privacy towards consumers and away from data holders.

II. BACKGROUND

This part of the Note will discuss the scope and contours of (1) the RTBF's European origin and its unsuccessful story in the United States; and (2) the RTD as established within the CCPA and subsequent U.S. state privacy bills. A contextual approach is necessary to distinguish the RTD from the RTBF and to map the similarities and differences between them. By distinguishing the two rights, it becomes clear that the act of deletion serves a different purpose within each right. Whereas the RTBF views the act of

5. *E.g.,* Yaki Faitelson, *Why 'Right to Delete' Should Be On Your It Agenda Now*, FORBES: TECH COUNCIL (Oct. 22, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/10/22/why-right-to-delete-should-be-on-your-it-agenda-now/?sh=5f7382a31b7f [https://perma.cc/FX3Y-5MXJ] ("In 2020, the [California Consumer Privacy Act] will give consumers some of the same rights as the [European Union's General Data Protection Regulation], including the right to delete personal information on demand."). *But see* Regulation 2016/679, of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 43-44 [hereinafter GDPR] (providing for the "Right to erasure ('right to be forgotten')"). The GDPR conflates the two rights by including the RTBF within the title of the right to erasure, which gives a consumer "the right to obtain from the controller the erasure of personal data concerning him or her without undue delay." *Id.* at 43. With each repetition of the privacy rights established by the GDPR, this conflation of two distinct rights has grown. *See, e.g.*, *Right to Erasure*, INFO. COMM'R'S OFF. (UK), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ [https://perma.cc/JQ6F-KZBM] (last visited Apr. 11, 2022) ("The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as the 'right to be forgotten.'").

deletion as a mechanism to achieve the substantive goal of digitally forgetting data (akin to human memory's natural retention limitation), the RTD views the act of deletion as the goal itself in order to empower greater consumer control over one's personal data.

A. The Right to Be Forgotten

1. The European Origins of the Right to Be Forgotten

The ambiguity of distinguishing between the RTBF and the RTD is in part due to terminology used to describe the evolution of the RTBF prior to (and during) the digital age. As recently as 2010, a European Commission Communication described the RTBF as "the right of individuals to have their data no longer processed *and deleted* when they are no longer needed for legitimate purposes."[6] The RTBF addresses the indefinite retention of digital information to theoretically grant a "dimension of oblivion, granting individuals a 'fresh start.'"[7] A natural tool to redress this harm is data deletion, whether cyclical and automatic or on an ad hoc and individual basis. The animating policy argument is that in the digital age, society must actively delete (and thus forget) information in order to mitigate the societal consequences created by external memory, which makes it cheaper to remember than to forget.[8] This need, advocates argue, has been amplified with trends such as "smart" devices extending from TVs, to doorbells, to lightbulbs that can integrate into Google Home-, Siri-, or Alexa-enabled networks.[9] To address this data permanence and restore digital memory to levels comparable to pre-digital society levels, digital storage devices (e.g., cameras, cellular devices, or computers) "should automatically delete information that has reached [a designated] expiration date."[10]

The RTBF itself can be traced to French law, which recognizes *le droit à l'oubli* (the "right of oblivion," which allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration),[11] as well as the Italian *diritto all'oblio* (which has been described as "the right to silence on past events in life that

6. European Commission Communication COM/2010/0609, A Comprehensive Approach on Personal Data Protection in the European Union (Nov. 4, 2010) (emphasis added).

7. Aurelia Tamò & Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 J. INTELL. PROP., INFO. TECH. & E-COM. L. 71, 73 para 17 (2014).

8. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 169 (2011).

9. Adam Levin, *Selling Privacy: The Next Big Thing for Entrepreneurs*, INC. (Dec. 5, 2019), https://www.inc.com/adam-levin/selling-privacy-next-big-thing-for-entrepreneurs.html [https://perma.cc/CF9H-X4LS].

10. Stuart Jefferies, *Why We Must Remember to Delete – and Forget – in the Digital Age*, GUARDIAN (June 30, 2011, 3:30 PM) https://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age [https://perma.cc/L8NG-BJQX].

11. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012).

are no longer occurring").[12] Similar rights developed in the jurisprudence of other European countries over the 20th century. In the United Kingdom, for example, the Rehabilitation of Offenders Act of 1974 reflects a principle of this right in the rehabilitation of past offenders.[13]

The RTBF, while not explicitly stated, can also be found by implication in various German legislation and jurisprudence. In 2013, German courts found that the RTBF, as an extension of the modern right to data protection under the Data Protection Directive of 1995, could be sourced not only from the idea of privacy, but also the German constitutional right to self-determination.[14] Specifically, the German Constitution guarantees that "every person shall have the right to free development of his personality."[15] Prior to the Data Protection Directive, in 1984, the Federal Labor Court linked the constitutional right of self-determination to the conventional European RTBF.[16] The court addressed whether a person had a "right to erasure of data that the data subject had disclosed himself" and held that a "job applicant's right to informational self-determination would be violated if a company who denied the applicant kept his or her data indeterminately."[17] The Federal Labour Court's ruling built on the decision in "*Lebach I*," where the German Federal Constitutional Court in 1973 reviewed a challenge by a murder convict against a television station for a documentary production that allegedly impinged the plaintiff's rights of personality and self-determination.[18] The court was asked to balance two competing constitutional rights: (1) the "freedom of the media under Article 5 of the Basic Law," and (2) the "personality rights of the convicted criminal under Article 2."[19] In *Lebach I*, the court held the encroachment of freedom of information "should not go any further than required to satisfy what was necessary to serve the public interest," opining that reports of events long since passed have less public interest if they pose new disproportional risks and "endanger[] the social rehabilitation of the criminal who has" a conviction.[20]

In 1995, the European Council passed Directive 95/46/EC (the "Directive") regarding the "protection of individuals[']… processing of

12. Giorgio Pino, *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, *in* THE HARMONISATION OF EUROPEAN PRIVATE LAW 225, 236 (Mark Van Hoecke & François Ost eds., 2000).

13. Rehabilitation of Offenders Act, (1974) c. 53, pmbl. (Eng.) ("An Act to rehabilitate offenders who have not been reconvicted of any serious offence for periods of years, to penalise the unauthorised disclosure of their previous convictions, to amend the law of defamation, and for purposes connected therewith.").

14. Claudia Kodde, *Germany's 'Right to Be Forgotten' - Between the Freedom of Expression and the Right to Informational Self-Determination*, 30 INT'L REV. L., COMPUTS. & TECH. 17, 19 (2016).

15. GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [CONSTITUTION] May 8, 1949, art. 2, § 1 (Ger.).

16. Kodde, *supra* note 14, at 27.

17. *Id.*

18. *Id.* at 26.

19. Nicole Jacoby, *Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 35 GA. J. INT'L & COMPAR. L. 433, 463 (2007).

20. Kodde, *supra* note 14, at 26.

personal data."[21] The Directive did not expressly include the right to be forgotten. Nonetheless, in 2014, the Spanish High Court asked the Court of Justice of the European Union ("CJEU") to determine "the scope of the right of erasure and/or the right to object, in relation to the '*derecho al olvido*' ("RTBF")" under the Directive.[22] In *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos* (*AEPD*) *and Mario Costeja González* (hereafter "*Google Spain*"), the CJEU considered whether the Directive created a right of erasure of true (but prejudicial) information that the subject "wishes . . . to be 'forgotten' after a certain time."[23] In the original complaint, Mr. González argued that under the Directive, "fundamental rights to the protection of those data and to privacy—which encompass the 'RTBF'—override the legitimate interests of the operator of the search engine and the general interest in freedom of information."[24] The CJEU found that the Directive's fundamental privacy rights included the right of a private citizen to request that his or her private name be removed from lists of "links to web pages published lawfully by third parties and containing true information relating to him."[25] The CJEU further found that this right overrides "the economic interest of the operator of the search engine [and] also the interest of the general public in finding that information upon a search relating to the data subject's name."[26]

The case has been studied by commentators both broadly and narrowly, and it illustrates the technical and legal ambiguity of key terms such as: forget, erasure, de-list, and delete.[27] On a narrow interpretative scale, *Google Spain's* holding was limited to processor obligations "to remove links to web pages" or to de-list.[28] Narrow-holding interpreters would state that the court explicitly did not find "that a 'RTBF' exists" and that it would be "misleading" to read in a RTBF outside of situations where "the data processing is incompatible with the Directive."[29] For those advocating a broad interpretation, *Google Spain* was a "ground-breaking" opening salvo. [30] In this interpretation, the court's decision to recognize an extensive RTBF that includes the "deletion or erasure of information that a data subject has disclosed passively" was "hardly surprising."[31]

---

21. Directive 95/46, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

22. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶ 20 (May 13, 2014).

23. *Id.* at ¶ 89.

24. *Id.* at ¶ 91.

25. *Id.* at ¶ 89.

26. *Id.* at ¶ 97.

27. *See, e.g.*, Orla Lynskey, *Control over Personal Data in a Digital Age:* Google Spain v. AEPD and Mano Costeja Gonzales, 78 MOD. L. REV. 522, (2015) (for a narrow interpretation); Amy Lai, *The Right to Be Forgotten and What the Laws Should/Can/Will Be: Comparing the United States and Canada*, 6 GLOB. J. COMPAR. L. 77, (2017).

28. Lynskey, *supra* note 27, at 522.

29. *Id.* at 528.

30. Lai, *supra* note 27, at 78.

31. *Id.* at 84, 80.

Even parties to the case characterized the holding differently in the aftermath. For instance, the European Commission's fact sheet about the *Google Spain* case described the Court's ruling as "[o]n the RTBF,"[32] while citing Article 17 (the right to erasure) and detailing the scope of a "request for erasure" as balanced against freedom of expression.[33] In contrast, Google's legal help support page refers to the RTBF as an obligation on processors to "delist certain results for queries" with no mention of obligations to adhere to data erasure requests,[34] while Google's current Transparency Report references the CJEU 2014 ruling without ever using the words "erasure" or "forget."[35] Both sources in unison undermine the clarity of the case's true holding and obfuscates the differences between the RTBF and the right to erasure (the right to delete in the United States).

2. A Rough Landing: The Right to be Forgotten in the United States

Two American cases, both contemporaries of *Google Spain*, demonstrate the uphill battle that litigants seeking to apply the RTBF face in the United States. First, in *Garcia v. Google*, actress Garcia brought a copyright action against YouTube's parent company, Google.[36] Garcia had responded to a casting call and read two lines of script; her voice was later over-dubbed with new lines and incorporated without her knowledge into an entirely new "anti-Islam polemic renamed *The Innocence of Muslims*."[37] A cleric subsequently issued a religious decree against those involved in the polemic.[38] Garcia, in fear for her safety, sought to have *The Innocence of Muslims* removed from YouTube or, in the alternative, have her lines cut from the footage.[39] To do so, she sought an injunction under a copyright theory of harm.[40] On review of a temporary injunction previously granted by a Ninth Circuit panel, the Ninth Circuit, sitting *en banc*, struck down the copyright-based injunction, noting that "[p]rivacy laws, not copyright, may offer remedies" tailored to Garcia's personal and reputation harms.[41] However, the *en banc* court declined to offer a "substantive view" of such an application of

32. EURO. COMM'N, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12) 1 (2014), https://web.archive.org/web/20140708142544/http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/J5LC-K3DC].

33. *Id.* at 4.

34. *Right to Be Forgotten Overview*, GOOGLE LEGAL HELP, https://support.google.com/legal/answer/10769224 [https://perma.cc/SPA4-E339] (last visited Jan. 26, 2022).

35. *Request to Delist Content Under European Privacy Law*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/N78B-Z3B6] (last visited Jan. 26, 2022).

36. Garcia v. Google, Inc., 786 F.3d 733, 738 (9th Cir. 2015) (en banc).

37. *Id.* at 737.

38. *Id.* at 738.

39. *Id.* at 738-39.

40. *Id.* at 745.

41. *Id.*

privacy law.[42] Further, the court noted that while "Garcia would like to have her connection to the film forgotten and stripped from YouTube," the RTBF, "although recently affirmed by the Court of Justice for the European Union, is not recognized in the United States."[43]

Second, in *Martin v. Hearst Corp*, an individual in a defamation and erasure case sought to have an article that reported on her arrest removed from a publication's website.[44] The State of Connecticut had previously dropped the charges under a *nolle prosequi* agreement, and the "arrest records were erased pursuant to [Connecticut's] Erasure Statute."[45] The individual argued that continued publication of the article was "false and defamatory" because "by the Erasure Statute, she was 'deemed to have never been arrested . . . with respect to the proceedings so erased.'"[46] In denying the cause of action, the Second Circuit interpreted the state erasure statute to establish only a "legal fiction . . . [that] bars the government from relying on the defendant's erased police, court, or prosecution records"; moreover, the presence of the erasure statute within the State's criminal code, as opposed to the civil code, demonstrated the legislature's intent for the statute not "to provide a basis for defamation suits."[47] As "there [was no] dispute that the articles published . . . accurately reported" the arrest, the "various publication-related tort claims necessarily fail[ed]" as a matter of law.[48]

A prevailing criticism against an expanded RTBF in the United States is its potential to disrupt or even harm journalistic endeavors, free speech, and the preservation of records.[49] An empowered RTBF could grant both the "right to suppress unpleasant lies which are publicly told" and may be "extended to unpleasant truths" told about individuals while those individuals are still alive.[50] Further, this disruption to online speech and records can limit natural online discourse.[51] Such criticisms have heightened energy in the United States due to the strong First Amendment protections that some argue are incompatible with the RTBF, while others argue that compatibility is

42. *Garcia*, 786 F.3d at 745.
43. *Id.*
44. Martin v. Hearst Corp., 777 F.3d 546, 548 (2d Cir. 2015).
45. *Id.* at 549.
46. *Id.*
47. *Id.* at 550.
48. *Id.* at 552.
49. *See* David Mitchell, *The Right to Be Forgotten Will Turn the Internet into a Work of Fiction*, GUARDIAN (July 5, 2014, 7:05 PM), https://www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google [https://perma.cc/DXQ2-KKK2] (suggesting that the right to be forgotten could undermine the Internet's value to leave for future historians "millions of searchable written sources" for posterity); *see also* James L. Gattuso, *Europe's Latest Export: Internet Censorship*, WALL ST. J. (Aug. 11, 2015, 6:50 PM), http://www.wsj.com/articles/europes-latest-export-internet-censorship-1439333404 [https://perma.cc/D6ZJ-SNKJ].
50. Mitchell, s*upra* note 49.
51. Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. POL'Y 91, 106-08 (2013).

clearly possible.[52] The First Amendment protects freedom of both speech and the press;[53] reflecting the inter-relatedness of both, the media is presumed to have unabridged access to "cover the truth and report it" about "government and public affairs [and] the truth about people."[54] While it is understandable that individuals might wish to be judged on current events rather than past events, in a "free speech regime," external views of a person "should primarily be molded by [readers'] own judgments"[55]—a dynamic potentially at risk when a person can use the RTBF to "keep them in the dark."[56]

However, recent literature has argued that it is possible to accommodate both freedom of speech and the RTBF in the United States. First, there is not an absolute tension between the RTBF and the First Amendment since American law has incorporated elements of the revisability principle—"the opportunity to revise one's beliefs and identity"—and placed it "at the very core of the reason we protect the freedom of expression."[57] Second, "[t]he media portray[al of the] conflict as a clash of two individual rights—the right to be forgotten or, more generally, the right to privacy versus the freedom of speech,"—is flawed.[58] Such an account "masks a far more diverse set of

52. *E.g.,* Farhad Manjoo, *'Right to Be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [https://perma.cc/CF85-RVQW] (covering divergent views of the First Amendment's implication on the adoption of the RTBF). An opponent of the RTBF argued that "altering the historical record or making information that was lawfully public no longer accessible to people" is challenging to "square [] with a fundamental right to access to information." *Id.* An advocate of the RTBF countered that "there were ways to limit access to private information that would not conflict with free speech," citing existing processes for the "global removal of some identifiable private information, like bank account numbers, social security numbers and sexually explicit images uploaded without the subject's consent." *Id.*

53. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . .").

54. David A. Anderson, *The Failure of American Privacy Law*, *in* 4 PROTECTING PRIVACY: THE CLIFFORD CHANCE LECTURES 139, 140 (Basil S. Markesinis ed.,1999).

55. Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1093 (2000).

56. *Id.*

57. Andrew Tutt, *The Revisability Principle*, 66 HASTINGS L.J. 1113, 1120 (2015). The "revisability principle" can also be found in the American traditions and values pioneers who sought second chances and reinvention. *See* Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. INFO. POL'Y' 1, 8 (2013) ("A long history of 'going West' has resulted in appreciation for loosening the shackles of one's past. Reputation is actively protected through mechanisms like defamation and the privacy torts of false light, public disclosure of private facts, intrusion upon seclusion, and misappropriation. Information flow is controlled through legal mechanisms like intellectual property laws and non-disclosure agreements."); *see also* Richard J. Peltz-Steele, *The 'Right to Be Forgotten' Online Is Really a Right to Be Forgiven*, WASH. POST. (Nov. 21, 2014), https://www.washingtonpost.com/opinions/the-right-to-be-forgotten-online-is-really-a-right-to-be-forgiven/2014/11/21/2801845c-669a-11e4-9fdc-d43b053ecb4d_story.html [https://perma.cc/7JFM-YF9T] (describing the RTBF as "really a right to be forgiven; a right to be redeemed; or a right to change, to reinvent and to define the self-anew," and stating that "there could be nothing more American than a second chance in a new world").

58. Edward Lee, *The Right to Be Forgotten v. Free Speech*, 12 I/S: J.L. & POL'Y FOR INFO. SOC'Y 85, 86 (2015).

responses countries can adopt in trying to reconcile the potential conflict."[59] For instance, "the First Amendment is no bar to voluntary industry practices (such as movie ratings and rape shield policies to protect the identities of rape victims)."[60] Further, in countries that have not recognized the RTBF as a matter of law, private companies, such as Google, could recognize the right "in their policies, practices, or technological design."[61]

B. The Right to Delete

1. The Right to Delete as Discussed Before the California Consumer Privacy Act

The technical interchangeability of words such as "erasure" and "delete," as well as the ambiguity surrounding the RTBF during its development, makes mapping the origin of the modern right a challenge. The concept of a "right to delete" has been previously articulated as an implied Fourth Amendment privacy right in the context of a remedy against digital mapping.[62] The right can be viewed as a remedy from a property rights lens: "[i]f imaging is neither search nor seizure, [then] law enforcement agents would have the incentive to image every hard drive they could find" without fear of a Fourth Amendment violation.[63] Advocates of this privacy interest view the Fourth Amendment as "broad enough to protect [a] 'right to destroy' or, in a computer context, [a RTD]" to mitigate the Fourth Amendment evasion of digital copying where the original "physical" property has not be dispossessed.[64]

The RTD as an alternative to the RTBF in the United States could shift the focus away from broad objectives, such as societal forgetfulness and oblivion and towards the idea of personal control over one's data. This removes some tensions with other liberty interests such as freedom of the press. One proposed RTD framework includes four categories of exceptions to an otherwise absolute right to delete: "conflicts with freedoms of speech and of the press; interactions with the right to contract; records associated with multiple individuals; and situations where deletion is impossible, infeasible, or socially harmful."[65] The RTD would further the overachieving privacy regime centered around consumer control and move away from a focus on consumer protection reflected in privacy regulatory elements, such as the minimization principle, which requires a data processor to "delete

59. *Id.*
60. *Id.* at 87.
61. *Id.* at 103.
62. Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10, 11 (2005).
63. *Id.* at 13.
64. *See id.* at 14.
65. Chris Conley, *The Right to Delete*, AAAI SPRING SYMPOSIUM: INTELLIGENT INFORMATION PRIVACY MANAGEMENT 53, 54 (2010), https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482 [https://perma.cc/GH94-BUAU].

unwanted information."[66] Principles such as minimization in support of a RTD help to shift the balance from data holders to data subjects and consumers. Rules providing "practical ways for users to access, modify, and/or delete their data," create a "feel[ing of being] in control," and such "[c]ontrol brings trust" between all involved parties.[67]

2. The Right to Delete as Shaped by the California Consumer Privacy Act

In 2018, California passed a comprehensive state general privacy law.[68] The CCPA provisioned a number of new consumer rights that reflected frameworks for privacy control mechanisms, such as rights of access, correction/modification, and the right (or privacy mechanism) of deletion. The statute gives consumers "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[69] The CCPA attaches several obligations on businesses that collect consumer data. First, a business must disclose "the consumer's rights to request the deletion of the consumer's personal information."[70] Second, the businesses shall "reasonably verify" that a request to delete comes from a person authorized to make such a request.[71] Upon receipt of a verified request, the company "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records."[72] While the verification step is arguably a procedural exemption, the CCPA also established a number of specific exemptions limiting the reach of a verified deletion request. For example, the CCPA would limit reach when execution would: impact certain business activities, such as detection of security incidents or activities "within the context of a business' ongoing business relationship with the consumer"; impair "[e]ngage[ment] in public or peer-reviewed scientific, historical, or statistical research in the public interest"; or would prevent a business from "comply[ing] with a legal obligation."[73]

The definition of "personal data" and the activity qualifier "collected from the consumer" limits the scope on the CCPA's consumer right of deletion. While the CCPA provides a broad list of data types that are included in the definition of personal data—from consumer identifiers to biometric

66. EU AGENCY FOR CYBERSECURITY (ENISA), PRIVACY BY DESIGN IN BIG DATA: AN OVERVIEW OF PRIVACY ENHANCING TECHNOLOGIES IN THE ERA OF BIG DATA ANALYTICS 26 (2015), https://www.enisa.europa.eu/publications/big-data-protection/@@download/fullReport [https://perma.cc/8VYR-6KEY].

67. *Id.* at 19-20.

68. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/4A8N-BZHS].

69. CAL. CIV. CODE § 1798.105(a) (West 2020).

70. CIV. § 1798.105(b).

71. CIV. § 1798.140(y).

72. CIV. § 1798.105(c).

73. CIV. § 1798.105(d)(1)-(9).

information and internet activity[74]—it also excludes a broad category of data, namely publicly available information ("PAI").[75] Lastly, the RTD is inapplicable against certain sectorial institutions or institutions that collect certain categories of data such as medical/health information,[76] consumer reporting information,[77] or financial information.[78]

In 2021, Virginia passed its state-wide general privacy act, the Virginia Consumer Data Protection Act ("VCDPA"),[79] followed soon after by the Colorado Privacy Act ("CPA").[80] While the VCDPA and CPA are not identical to the CCPA, all three share broad structural similarities such as the creation of various consumer rights, obligations on data-holders (processors and/or controllers), and technical privacy control mechanisms.[81] All three statutes include a consumer RTD.[82] The VCDPA grants a consumer, or other authorized party, the right to "delete personal data provided by or obtained about the consumer."[83] The VCDPA grants controllers the same procedural exemption to comply with a request only if a controller can "authenticate the request using commercially reasonable efforts."[84] The VCDPA excludes from the definition of personal data "de-identified data or publicly available information."[85]

The CPA provides consumers "the [RTD] personal data concerning the consumer."[86] Mirroring the VCDPA, the CPA provides that controllers are "not required to comply with a request" if they are "unable to authenticate the request using commercially reasonable efforts, in which case the controller may request the provision of additional information reasonably necessary to authenticate the request."[87] The CPA defines personal data as "information

74. CIV. § 1798.140(o)(1).

75. CIV. § 1798.140(o)(2). In 2020, the California Privacy Rights Act (CPRA) amended the definition to also exclude consumer information that "is deidentified or aggregate consumer information." CIV. § 1798.140(o)(3).

76. CIV. § 1798.145(c)(1).

77. CIV. § 1798.145(d).

78. CIV. § 1798.145(e).

79. Christopher Escobedo Hart & Colin Zick, *Virginia's New Data Privacy Law: An Uncertain Next Step for State Data Protection*, JD SUPRA (July 7, 2021), https://www.jdsupra.com/legalnews/virginia-s-new-data-privacy-law-an-8812636/ [https://perma.cc/SRA5-VHHM]. For a comparison of each state act's right to delete, see Glenn A. Brown, *Consumers' "Right to Delete" Under US State Privacy Laws*, SQUIRE PATTON BOGGS (Mar. 3, 2021), https://www.consumerprivacyworld.com/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/ [https://perma.cc/JHJ5-J4GA].

80. Hannah Schaller et al., *Colorado Enacts New Consumer Privacy Law*, ZWILLGEN (Aug. 3, 2021) https://www.zwillgen.com/privacy/colorado-privacy-act/ [https://perma.cc/MDJ8-NHVT].

81. For a more in-depth comparative analysis of the three acts, see Cathy Cosgrove & Sarah Rippy, *Comparison of Comprehensive Data Privacy Laws in Virginia, California and Colorado*, INT'L ASSOC. PRIV. PROFS. (July 8, 2021), https://iapp.org/resources/article/comparison-comprehensive-data-privacy-laws-virginia-california-colorado/ [https://perma.cc/N8BZ-54YW].

82. *Id.*

83. VA. CODE ANN. § 59.1-577(A)(3) (West 2021).

84. § 59.1-577(B)(4).

85. § 59.1-575.

86. COLO. REV. STAT. ANN. § 6-1-1306(1)(d) (West 2021).

87. § 6-1-1306(2)(d).

that is linked or reasonably linkable to an identified or identifiable individual" and "does not include de-identified data or publicly available information."[88]

C. *Contrasting the Right to be Forgotten and the Right to Delete*

Both the RTBF and the RTD are concerned with the "protect[ion of] privacy and self-determination interests in the context of permanent memory."[89] But, as an alternative to the RTBF's broad automatic deletion over time approach, the RTD provides consumers the ability to delete "certain records from any permanent repository."[90] Thus, the RTD would grant persons more individualized "control over personal records" than the RTBF would.[91]

The RTBF focuses on addressing the digital retention of information in a new age, the consequences of which affect an individual's rights to privacy and self-autonomy; deletion is a means to an end only, and it is not the focus of the right. The RTD addresses different policy goals, and while the adoption of a RTBF in the United States might overlap with those goals, it would not necessarily further the objectives of the RTD. It is notable that recent state privacy laws include the RTD, while the older RTBF has struggled to gain minimal traction and adoption within the United States, despite the two rights' adjacent policy aims.

For the purposes of this discussion, this Note proposes that there are four salient differences between the RTBF and RTD: (1) the core power each legal right seeks to bestow on individuals; (2) the type of data targeted; (3) the relationship targeted; and (4) the technical implementation of each right.

First, while a RTBF grants the power of anonymity over time, the RTD is focused on empowering data objects with some degree of control over their personal data with respect to the data itself and its holders. "Control" means "to direct" or "to have power over" something, and in this case, indicates a consumer's ability to exercise some measure of power over, and influence the use of, their data held by another party.[92] While this control provides a person the power to *potentially* effectuate a given result, it does not ensure it. This is different from the RTBF, which focuses on the concept of automatic deletion over time to replicate long-term human memory loss.[93] If a person controls their data under a RTD regime, they could submit a deletion request; however, they may choose not to for a variety of reasons, such as indifference to the possession of the data by another party, an ongoing economic relation, or even the efficiency of resuming an ongoing relationship in the future.

88. § 6-1-1303(17)(a)-(b).
89. Conley, *supra* note 65, at 54.
90. *Id.*
91. *Id.* at 57.
92. *Control*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/control [https://perma.cc/QY7P-MCSW] (last visited Feb. 1, 2022); *see also Control*, BLACK'S L. DICTIONARY (11th ed. 2019) ("To exercise power or influence over.").
93. Jefferies, *supra* note 10.

Second, the RTBF targets broad narratives a party seeks to have removed from *society's* digital memory.[94] In contrast, the RTD is content-neutral in its potential scope, and a party may seek to delete aggregate data that may collectively establish a narrative or target smaller or, on the other hand, specific types of information they simply no longer wish a data holder to have. This can happen for any variety of reasons, such as minimizing how many vendors have their email address or cellphone number. If the RTBF reflects societal values between an individual and their community at large, the RTD reflects a societal goal of allowing individual market participants to exit at any time—but to exit cleanly requires deletion of one's personal data given to a service provider.

Third, as the RTBF focuses on the erasure of narratives, the right itself is concerned with the relationship between an individual and society at large—even when a dispute is between two private parties (in this case, an individual and a data holder). The data holder is the target of the erasure request, but the relationship impacted is between the individual and the community's view of them. Here, the RTD starkly diverges, as the relationship impacted is nearly entirely between two private parties in a transactional sense with no wider societal implication.

Lastly, the RTBF and the RTD are different in their technical implementation. The RTBF can be achieved in a number of ways, but the most commonly-advocated methods are either requiring automatic erasure—creating a digital clock to replicate the non-digital nature of memory to all data—or other measures, such as de-listing, as held in *Google Spain*.[95] In the first case, such a technical rule is a single rule for all personal data. In the second case, a de-listing request interrupts the ability for a local community to find a past, and *now forgotten* narrative of one of its own, even if the narrative itself is retained somewhere online. In contrast, a deletion request under the RTD targets the data itself at its final stored location and has a greater sense of finality than de-listing. Additionally, reflecting the policy goal of granting a consumer control, a deletion request under the RTD is ad hoc, may be made at any time, and may only target a fraction of the data held by the data holder.[96] At the aggregate level, such an ad hoc nature is random in comparison to a RTBF automatic timer.

---

94. *E.g.,* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 14-15 (May 13, 2014) (where Mr. Gonzales sought to have the narrative of his past financial foreclosures forgotten as part of his present self's re-invention); *see generally* Kodde, *supra* note 14, at (where the information targeted for deletion was generally descriptive information such as a name, background information, gender, past work experience, etc., but the narrative targeted was one of a denied job application that the petitioner sought to prevent from impacting future job search prospects); *see also* Martin v. Hearst Corp., 777 F.3d 546, 548-49 (2d Cir. 2015) (where in the United States, the plaintiff, while denied, sought to fully close the chapter of a past arrest without conviction and remove the narrative from her present-day life and community). For further discussion on narratives, *see* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, PRIVACY ON THE INTERNET 15-102 (2007).

95. *Supra* text accompanying notes 21-25.

96. *Supra* text accompanying note 66, and II.B.2.

III. ANALYSIS

Having distinguished the RTD from the RTBF, the next question is how effective the RTD is at achieving a privacy rights regime's intended goals. As the first RTD was enacted only four years ago, there is negligible quantifiable data or cases to objectively measure its impact.[97] Instead, while an objective or quantifiable study might not yet be feasible, a qualitative analysis of the RTD's limitations and structure—from its procedure and exceptions to other drafting provisions—is possible. This qualitative analysis allows for reforms now, while the right is still in its infancy and yet to be widely adopted across the United States.

A. The Harm of No Standard Technical or Legal Definition of "Delete"

When a consumer exercises their RTD and submits a request to a company, they probably think that their data will be deleted permanently and irretrievably, and that this standard of deletion is uniform across state privacy laws. This consumer presumption is likely incorrect, and typically, "a user's commonsense understanding of the command to 'delete' differ[s] from companies' practices."[98] Beyond consumers, "employees who would be trusted to carry out these technical [deletion & data disposal] tasks often lack basic training on how to do them."[99] Legislators seeking to improve the efficiency of the RTD and strengthen its impact should better regulate and define deletion standards for covered entities. There are three main obstacles to resolving ambiguities on what deletion standard is owed to a consumer: (1) the lack of uniform data deletion and disposal standards; (2) the RTD's interaction with a legal regime that, by design and incentive, prefers data retention; and (3) the variance of technical deletion methods and the financial burden of different deletion methods.

97. Early signs show a low usage of the RTD under the CCPA, with a relatively small number of annual requests submitted so far against the majority of Fortune 500 companies. *See* David A. Zetoony, *How Many Deletion Requests Do Retailers Receive on Average Each Year*?, GREENBERG TRAURIG (Sept. 13, 2021), https://www.gtlaw-dataprivacydish.com/2021/09/how-many-deletion-requests-do-retailers-receive-on-average-each-year/ [https://perma.cc/PX6N-ARCQ]. The vast majority of requests targeted at most only three companies. *Id.*

98. MICHELLE DE MOOY ET AL., CTR. FOR DEMOCRACY & TECH., THE LEGAL, POLICY AND TECHNICAL LANDSCAPE AROUND DATA DELETION 3 (2017), https://cdt.org/wp-content/uploads/2017/02/2017-02-23-Data-Deletion-FNL2.pdf [https://perma.cc/52JZ-R6DY].

99. *Id.* at 6; *see also* Thomas Brewster, *500 Million Google Phones Fail to Wipe Data on Reset, Claim Cambridge Researchers*, FORBES (May 22, 2015, 10:31 AM), https://www.forbes.com/sites/thomasbrewster/2015/05/22/google-android-phones-fail-to-delete-data-on-reset/ [https://perma.cc/6GXT-D7QT].

1. There is No Standard Legal Rule Governing Deletion and Data Disposal

The majority of states have enacted some form of data disposal laws (though some have not been passed or amended recently).[100] Already, there is inconsistency across bills as to whether the controlling data disposal laws apply to both businesses and government,[101] businesses but not to government,[102] or only to government and not to business.[103] Since the RTD is now law in at least three states,[104] the standard for a deletion request by a consumer or covered entity is the corresponding state records and disposal law.

The California data disposal law, as amended in 2009, states that:

> A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.[105]

While the disposal provision provides some specificity on the technical standard to be met (namely, rendering the data unreadable or undecipherable), it is also tied to a definition of "personal information," which may exclude data that a consumer assumes would be deleted and may also be inconsistent with the definition of "personal information" under the CCPA.[106] Consequently, the burden shifts to the consumer to research multiple provisions of two state laws to determine if the data they seek to have deleted is covered, the tedious nature of which is inconsistent with the RTD's emphasis on control and direction over one's own data by a consumer.[107]

In contrast to California, the Virginia data disposal law is far less controlling on what standard is required in response to a deletion request. First, the state's data disposal laws only require the Virginia Information

---

100. *Data Security Laws | Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (last updated May 29, 2019) https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector [https://perma.cc/XG5K-HW8Y] ("more than half the states also have enacted data disposal laws that require entities to destroy or dispose of personal information so that it is unreadable or indecipherable). For a list of state governmental disposal statutes *see Data Security Laws | Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (last updated May 29, 2019) https://www.ncsl.org/technology-and-communication/data-security-laws-state-government [https://perma.cc/8H8D-P9X8].

101. *E.g.,* ALA. CODE § 8-38-10 (2018); MICH. COMP. LAWS ANN. § 445.72(a) (West 2007).

102. *E.g.,* IND. CODE ANN. §§ 24-4-14-8, 24-4.9-3-3.5(d) (West 2021); NEB. REV. STAT. § 87-808(1) (West 2006).

103. *E.g.,* VA. CODE ANN. § 2.2-2009 (West 2020).

104. *Supra* note 1, and 4.

105. CAL. CIV. CODE § 1798.81 (West 2020).

106. CIV. § 1798.81.5.

107. *See supra*, II.C. Contrasting the Right to be Forgotten and the Right to Delete.

Technologies Agency Chief Information Officer ("CIO") to provide technical guidance regarding "the development of policies, standards, and guidelines," which can be changed by a subsequent CIO.[108] Second, the law and any CIO guidance applies only to the "Commonwealth's executive, legislative, and judicial branches and independent agencies,"[109] a narrower body of entities than those covered by the VCDPA's RTD. Thus, Virginia's data disposal law is both not controlling for RTD requests and is potentially subject to repeated changes from one CIO to another.

Colorado's code governing disposal of personal identifiable information ("PII") was amended in 2018 to include electronic documents and requires covered entities to develop policies for the destruction and disposal of records containing PII.[110] The Colorado regime, like the California disposal regime, applies broadly to covered entities but provides little specificity as to what constitutes proper disposal for electronic records containing PII.[111] Also like the California disposal regime, the Colorado governing rule has its own definition of PII and is at risk of subsequent inconsistencies between personal data covered under the CPA's RTD and the state's disposal rules.[112]

At the federal level, many authorities dealing with privacy, cybersecurity, data protection, and other substantive areas provide instructions, optional rules, and guidance concerning data disposal. For example, the Department of Health and Human Services ("HHS") has issued guidance on the disposal of protected health information pursuant to the

108. VA. CODE ANN. § 2.2-2009(F) (West 2020) ("The CIO shall provide technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as determined by the CIO, of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets.").

109. § 2.2-2009(I)(1).

110. COLO. REV. STAT. ANN. § 6-1-713(1) (West 2018) ("Each covered entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic documents containing personal identifying information. Unless otherwise required by state or federal law or regulation, the written policy must require that, when such paper or electronic documents are no longer needed, the covered entity shall destroy or arrange for the destruction of such paper and electronic documents within its custody or control that contain personal identifying information by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to make the personal identifying information unreadable or indecipherable through any means.").

111. *See* § 6-1-713.

112. *E.g.,* § 6-1-713(2)(b) (defining PII as a "social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in section 6-1-716(1)(a); an employer, student, or military identification number; or a financial transaction device as defined in section 18-5-701(3)").

HIPAA Breach Notification Rule.[113] The guidance deals not with data deletion itself, but rather provides a standard for rendering protected health information "unreadable, or indecipherable to unauthorized persons."[114] Electronic protected health information ("PHI") must be encrypted consistent with a standard approved by the National Institute of Standards and Technology ("NIST"); PHI stored on physical media (paper, film, or electronic media) must be destroyed by one method from an enumerated list.[115] In contrast to HHS's approach, the Federal Trade Commission ("FTC") has established a mandate for data disposal under the Fair and Accurate Credit Transactions Act ("FACTA").[116] However, while the FACTA disposal requirement is a mandate, it provides far less specificity on the standards for data disposal or deletion, only requiring covered persons or entities to "properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[117]

2. The Right to Delete is Opposed to the Core Design of Legal and Technical Data Disposal Rules

Legislators and policy makers should acknowledge that the RTD is inapposite to the current legal environment and technical design of systems governing data collection, storage, and processing. First, there is currently an inherent bias in favor of big-data collection and storage, as "[i]ncreasingly, data assets are the engine driving the total value and growth of modern

113. HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 (2009); *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/URL7-88TC] (last visited Nov. 14, 2022) ("Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.").

114. 45 C.F.R. § 164.402 (2009).

115. *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html [https://perma.cc/SPH5-3GQ9] (last visited Mar. 5, 2022); *see also What Do the HIPPA Privacy and Security Rules Require of Covered Entities When They Dispose of Protected Health Information?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Feb. 18, 2009), https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html [https://perma.cc/X8AS-ZLJR] (requiring that "workforce members receive training on . . . disposal policies and procedures . . ." and providing guidance on appropriate disposal standards, depsite the absence of a mandate for covered entities to dispose of PHI).

116. FTC Disposal of Consumer Report Information and Records, 16 C.F.R. pt. 682 (2007); *see also* Press Release, Fed. Trade Comm'n, FACTA Disposal Rule Goes into Effect June 1 (June 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1 [https://perma.cc/YF5Z-W4ZW].

117. 16 C.F.R § 682.3(a) (defining "Standard").

organizations."[118] Beyond the value of individual data profiles of consumers, companies see a myriad of big-data analytic opportunities to use aggregate consumer profiles for improved product and service performance, cost improvement, and new value and derived insights.[119] Consequently, entities covered by privacy statutes are typically incentivized by the market to maximize their digital data collection practices.

Second, numerous sectoral laws require companies to preserve records, from accounting and financial documents to other transactions for law enforcement and civil government administration.[120] Additionally, companies themselves have favored storage in preparation for potential litigation, as the rise in e-discovery costs demonstrates.[121] Unfortunately, historical focus has been on effective record management in preparation for future litigation, [122] rather than on what is essential to save and what is not. However, contrary to current data retention practices, the over-collection of data can "leave[] companies open to serious consequences."[123] One study found that only "one percent of data needs to be retained for litigation purposes," and that up to "70 percent of a company's data assets serve mostly to create liability."[124]

Third, online data use and storage disfavors deletion given the technical challenges of data erasure and the rise of built-in data retrieval technologies.[125] This issue extends from data collection and storage design to data sets themselves in machine learning and AI, where individual data

118. DELOITTE, DATA VALUATION: UNDERSTANDING THE VALUE OF YOUR DATA ASSETS 2 (2020), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Finance/Valuation-Data-Digital.pdf [https://perma.cc/Q5XE-2526].

119. *See* THOMAS H. DAVENPORT & JILL DYCHÉ, INT'L INST. FOR ANALYTICS, BIG DATA IN BIG COMPANIES 3 (2013), https://docs.media.bitpipe.com/io_10x/io_102267/item_725049/Big-Data-in-Big-Companies.pdf [https://perma.cc/B82V-VMFZ%5d].

120. *E.g.,* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 802, 116 Stat. 745, 800-01 (2002) (governing the record-keeping obligations of accounting and financial auditors).

121. John H. Beisner, *Discovering a Better Way: The Need for Effective Civil Litigation Reform*, 60 DUKE L.J. 547, 585 (2010) ("[T]he ubiquity of modern computer systems—and the ever-growing caches of information they contain—has led to a tremendous surge in the costs of electronic discovery.").

122. *See, e.g.*, Steven C. Bennett, *Records Management: The Next Frontier in E-Discovery*, 41 TEX. TECH L. REV. 519, 522 (2009) (analyzing how "[e]ffective [records management] can dramatically improve the e-discovery process," and how "[w]ell organized information can be more easily and cheaply gathered, searched, reviewed, and produced" and not how companies can efficiently delete non-essential data and preserve the truly relevant and required data).

123. DE MOOY ET AL., *supra* note 98, at 7.

124. *Id.*

125. Technology service providers often provide guidance or applications to recover files after a consumer has theoretically deleted them. *E.g., Recover Lost Files on Windows 10*, MICROSOFT, https://support.microsoft.com/en-us/windows/recover-lost-files-on-windows-10-61f5b28a-f5b8-3cc2-0f8e-a63cb4e1d4c4 [https://perma.cc/S8R4-ZT2V] (last visited Mar. 5, 2022); *Move Files to Trash and Restore Files from Trash*, FILES BY GOOGLE, https://support.google.com/files/answer/10607740 [https://perma.cc/D86W-M3HJ] (last visited Mar. 5, 2022).

deletion requests are particularly opposed.[126] This is related to the next critical issue the RTD faces, which is the difficulty in deletion itself and its various definitions and methods.

3. Technical Definitions and Methods of Deletion Vary

There are material differences between various technical and legal standards of deletion, particularly given inconsistent standards for responding to a deletion request. Traditional deletion methods for data held on individual devices include (1) the command delete, which "removes pointers to information on your computer, but . . . does not remove the information"; (2) overwriting, which "puts random data in place of your information . . . [that] cannot be retrieved because it has been obliterated"; and (3) physical destruction.[127] Further, some deletion standards and recovery tools focus on individual hardware data[128] and thus are likely inapplicable for the majority of covered entities who would receive a request. As data has migrated to cloud computing services, over-writing and other cryptographic erasure techniques[129] have become more prominent, with physical destruction only available for companies seeking to destroy an entire data set or asset. Google's Cloud system uses multiple deletion methods depending on the product or data marked for deletion.[130] Cloud-stored data is deleted through both cryptographic erasures and overwriting, where copies of the data are

126. *See* Antonio A. Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning*, *in* ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS 32: PROCEEDINGS OF THE 2019 CONFERENCE 3502, 3504-508 (Hanna M. Wallach et al. eds., 2019) (discussing the value of deletion efficiency within general learning algorithms and proposing two deletion efficient solutions).

127. LINDA PESANTE ET AL., U.S. COMP. EMERGENCY READINESS TEAM, DISPOSING OF DEVICES SAFELY 2 (2012), https://www.cisa.gov/uscert/sites/default/files/publications/DisposeDevicesSafely.pdf [https://perma.cc/7UEN-7G79].

128. For instance, there are deletion methods and recovery tools more focused on an individual device, such as a laptop or phone, that would likely be irrelevant to a data deletion request to a company which might store data via one or even many cloud-storage companies. One example is DiskDigger, a free tool that helps recover Windows files from a specific laptop and is often used in gathering forensic evidence by law enforcement. CHUCK EASTTOM, COMPUTER SECURITY FUNDAMENTALS 399 (Mark Taub et al. eds., 4th ed. 2020).

129. Cryptographic deletion is a two-stage process. First, data is encrypted in a procedure to "scramble information so that only someone knowing the appropriate secret [an encryption key] can obtain the original information . . . ." CHARLIE KAUFMAN ET AL., NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD (Faye Gemmellaro et al. eds, 2d ed. 2002). Second, during the erasure process, rather than overwriting data, the encryption key is erased using "similar overwriting methods." *Id.* The process prevents description of the data and requires overwriting of only data keys, a smaller volume to overwrite, than the full data itself. *See* Sarah M. Diesburg & An-I Andy Wang*, A Survey of Confidential Data Storage and Deletion Methods*, 43 ACM COMPUTING SURVS., no. 1, 2010, at 1, 4, 28.

130. *Data Deletion on Google Cloud*, GOOGLE CLOUD, https://cloud.google.com/docs/security/deletion [https://perma.cc/4F9M-A3BQ] (last visited Mar. 6, 2022).

marked as "storage and overwritten over time."[131] Amazon employs similar techniques but denotes data blocks (digital storage room) to be wiped only "immediately before reuse" which can give the appearance that something has been deleted when the act of deletion has yet to occur.[132]

4. Recommendations

In reviewing the legal and technical environment surrounding deletion, it is clear that (1) there is likely a disconnect between consumer understandings of deletion and legal deletion under state law and (2) consumers and covered entities have a myriad of authorities they must consult for guidance on both legal coverage and technical standards to execute data deletion requests under the RTD. Bridging the gap between consumers' expectations and reality and simplifying compliance for covered entities is essential for the RTD to be effective.

A starting point on the legal side of deletion is to adopt a more standardized definition. While this is a common refrain to privacy law reform discussions, it is particularly salient for deletion requirements considering the technical nature of compliance. First, legislators should harmonize the different approaches to deletion. This means that rather than states adopting different examples or standards to define "reasonable steps" for data deletion or record disposal, all states should consider adopting a single approach.[133] Second, legislators should ensure that the scope of their state privacy bills—from covered entities to the definitions of PII—match any equivalent controlling state data and records disposal laws. This would correct ambiguous gaps, such as in Virginia, where the disposal guidance is controlling only to governmental agencies and not to all entities covered under the VCDPA.[134] There is an inherent difficulty in aligning state rules and compliance, as individual states fiercely protect their own approach.[135] However, the RTD (perhaps more than the other rights under recent privacy bills) is normally focused on re-balancing the control between consumers and data-holders. The more difficult compliance is for companies that operate nationally, the more such a re-balance of control is undermined.

While improved consistency in legal standards is required, too much specificity is neither desirable nor reflective of the constant evolution of data

131. *Id.*

132. AMAZON WEB SERVS., OVERVIEW OF AWS SECURITY – COMPUTE SERVICES 7 (2016) [hereinafter OVERVIEW OF AWS SECURITY], https://d0.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf [https://perma.cc/NX2Z-7LNP].

133. *E.g.,* DEL. CODE ANN. tit. 19, § 736(b) (West 2015).

134. *See supra* notes 107-08 and accompanying text.

135. *E.g.*, Letter from Rob Bonta, Attorney General, State of California, and Nine Attorneys Generals to Congressional Leaders (July 19, 2022), https://cppa.ca.gov/meetings/materials/20220728_item2_letter_attorney_general.pdf [https://perma.cc/EXL8-49HC] (arguing against the proposed federal preemption of the 2022 American Data Privacy and Protection Act bill in contemplation by Congress and encouraging Congress to "adopt a federal baseline, and continue to allow states to make decisions about additional protections for consumers residing in their jurisdictions").

management and technology. A compromise for state legislators is to defer technical standards to an alternative body. NIST would be an ideal candidate for such an approach. NIST has substantial technical competency that would be difficult for state legislators to match in determining standards. More importantly, NIST has taken an enlarged role in recent years, having published guidance in the cyber, privacy[136] and computing environment. And many of the largest service providers already comply with NIST standards.[137] Such an approach would harmonize standards and technical competence and reduce compliance complexity for data holders operating under various privacy regimes and data deletion requests. An additional benefit of NIST standards is the flexibility they would provide to the range of covered entities. Deletion is not a binary process; it entails a range of methodologies that contain many tradeoffs.[138] Covered entities range in type and scale, and a one-size-fits-all approach to deletion may increase costs and difficulties for some organizations beyond the benefit provided to consumers. NIST is well-suited to mitigate this risk, as many of their standards reflect the disparate needs of organizations reliant on their guidance. For instance, both the NIST Cybersecurity and Privacy Frameworks create organizational profiles and menus of technical options and approaches reflective of the circumstances of individual organizations.[139] While states themselves might be reluctant to create a rights-based privacy regime dependent on a federal body they have no influence or control over, this approach might provide the most balanced improvement to RTD. Such an idea might be gaining traction, with one proposed state privacy bill already attempting to incorporate NIST standards into its regime.[140]

B. The Risk of De-identification Exemptions to The Right to Delete

Another area for legislators to address to improve the RTD is the risk of anonymization exemptions to deletion requests in the face of the progress made in re-identification science and methodologies. A common exemption to the scope of personal data—and any related rights that might turn on a

136. *See generally* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST 800-88, GUIDELINES FOR MEDIA SANITIZATION (2014), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [https://perma.cc/RCG5-BQBR].

137. OVERVIEW OF AWS SECURITY, *supra* note 131, at 7.

138. Diesburg & Wang, *supra* note 128, at 30.

139. *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0, 8 (2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf [https://perma.cc/PC4Z-CH4E]; NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 v-vi, 11 (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/JA76-KWPV].

140. *E.g.,* H.B. No. 376, 134th Gen. Assemb., Reg. Sess. § 1355.11(I)(1)(a)(i) (Ohio 2022) (proposing under the Ohio Personal Privacy Act an affirmative defense for a covered entity that "reasonably conforms to the [NIST] privacy framework").

definition of personal data or PII—is de-identified (also anonymized and/or pseudonymized) data.[141] Under the CCPA, a deletion request does not extend to personal data that is "deidentified or [converted to] aggregate consumer information."[142] Both the CPA and VCDPA contain the same de-identification exemption.[143] Historically, de-identification "has been the main paradigm used in research and elsewhere to share data while preserving people's privacy."[144] Unfortunately, regulators and "legal scholars share [a] faith in anonymization" that does not reflect recent trends and progress in re-identification science.[145]

De-identification as a free pass to deletion for business and data-processors, combined with "the power of reidentification[,] will create and amplify privacy harms" and potentially undermine the purpose of empowering consumers with more control over their personal data.[146] Even in the early 2000s, companies were relying on de-identification to expose private data under the gaze of external research, such as the AOL research data set that allowed for the re-identification of its data set objects who were users in the study.[147] Privacy regimes refer to de-identified data not in absolute terms, but as data that cannot be reasonably re-identified. The reality is that it is relatively easy to re-identify data. One recent study compared different methodologies of re-identification to determine the likely success of re-identification; crucially, the study found that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes."[148]

---

141. Provisions for de-identification exemptions and methods are common in federal laws and regulations. *See, e.g.*, OFF. FOR C.R., U.S. DEP'T OF HEALTH & HUM. SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 5-6 (2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf [https://perma.cc/C6NK-R6WS]; *see also* PRIV. TECH. ASSISTANCE CTR., U.S. DEP'T OF EDUC., DATA DE-IDENTIFICATION: AN OVERVIEW OF BASIC TERMS 3 (2012), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf [https://perma.cc/S749-P6VD].

142. CAL. CIV. CODE § 1798.140(v)(3) (West 2020).

143. *See* VA. CODE ANN. § 59.1-571 (West 2021); COLO. REV. STAT. ANN. § 6-1-1303(17)(b) (West 2021).

144. Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 NATURE COMM., no. 3069, 2019, at 1, 2.

145. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1710-11 (2010).

146. *Id.* at 1705.

147. Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html [https://perma.cc/2TKW-N7NF] (reporting that amongst other re-identification efforts, a single user was identified as an example of the privacy harm AOL's release of supposedly protected anonymized data had unleased).

148. Rocher et al., *supra* note 143, at 1; *see also Too Unique to Hide*, NATURE COMM., https://cpg.doc.ic.ac.uk/individual-risk/ [https://perma.cc/P5DR-36CN] (last visited Nov. 15, 2022) (featuring an online tool developed by the authors of the source in note 143 that allows U.S. and U.K. residents to test whether they can already be re-identified).

Without entirely blocking the value of anonymized data for researchers,[149] legislators must acknowledge that the protection level of de-identification is weaker than assumed and take a second look at how broadly such an exemption should apply to privacy rights, such as the RTD, in the context of truly empowering consumers to control their personal data.

C. An Alternative Path: Market Incentives To Collect & Retain Less Consumer Data

While the previous two sections focused on areas of improvement for the RTD, policymakers should also keep in mind the limitations to what the RTD can address. This Note has argued that the RTD can and should be strengthened, but ultimately it is only one right in a legal regime that focuses on providing consumers more measurable control over their personal data, which is distinct from wide-spread data protection.

Regardless of the policy goals of the RTD, "rights are often asked to do far more work than they are capable of doing."[150] Legislators and regulators should consider going beyond addressing gaps in the current design of the RTD and consider engaging with businesses directly to encourage practices that reduce the scope of data collected ahead of subsequent consumer deletion requests.

Going beyond strengthening privacy rights, there are three arguments that legislators and regulators can deploy in such deliberations with business or regulatory bodies that collect and store vast amounts of personal data. First, companies must embrace the paradigm shift that they *will* be breached and risk exposing their data assets and consumer personal data.[151] Businesses and governmental data-holding bodies cannot ignore their centrality in societal privacy protections and assume that they will not be drawn into the fray.[152] Second, *when* a cyber breach does occur, there is now a large body of authorities that govern the response, particularly the evidence and forensic gathering steps that breached organizations must adhere to. These range from

149. *See* CERT Podcast Series: Security for Business Leaders, *The Value of De-Identified Personal Data*, SOFTWARE ENG'G INST., at 07:50 (May 15, 2007), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34562 [https://perma.cc/DMC6-9K67] (transcript available for PDF download on linked webpage).

150. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023) (manuscript at 2) (on file at The George Washington University Law School Scholarly Commons, Paper Series 2022-30).

151. Tyler Anders et al., *Not "If" but "When"—The Ever Increasing Threat of a Data Breach in 2021*, JD SUPRA (July 15, 2021), https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/ [https://perma.cc/N7T5-J2BK] ("If the statistics are correct, the question for most companies is not if they will be a victim of cybercrime, but when.").

152. *See* CYBERSECURITY UNIT, U.S. DEP'T OF JUST., BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 1 (2018), https://www.justice.gov/criminal-ccips/file/1096971/download [https://perma.cc/F3TR-YUCR] (discussing the importance of "[h]aving well-established plans and procedures . . . to weather a cyber incident," with less of an emphasis on avoiding possible cyber breaches).

U.S. Secret Service guidance[153] to international law under the Budapest Convention (to which the United States is a party).[154] As previously discussed, when a breach occurs, there is often extensive e-discovery and litigation costs,[155] amplified by the volume of data needlessly exposed because of over-collection and retention practices by firms, which the RTD cannot solve by itself.

Third, to manage this increased liability, there are non-regulatory solutions that firms can employ, whether they decide to collect and retain less data to address privacy harms[156] or are self-incentivized to reduce extremely likely future litigation costs. Organizing vast data sets and deleting irrelevant or low-value data without decreasing the value of a businesses' data assets is possible and desirable.[157] Organizations should look internally to develop or employ newly available tools to reverse track from the existing absolutism that more data is better.

IV. CONCLUSION

Understanding the backgrounds of the RTBF and RTD is critical to distinguishing the two rights and analyzing problems with the RTD. Some of the debate and analysis of the RTBF can be drawn on when analyzing the RTD, but it is ultimately not controlling. The RTD has the potential to help shift the balance of control over one's personal data, but in its current form, will have only a limited effect. A more effective RTD that applies uniformly

---

153. U.S. SECRET SERV. CYBERCRIME INVESTIGATIONS, PREPARING FOR A CYBER INCIDENT: AN INTRODUCTORY GUIDE (2020), https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20An%20Introductory%20Guide%20v%201.1.pdf [https://perma.cc/BH98-3QFB].

154. The Budapest Convention on Cybercrime, passed by the Council of Europe, discusses electronic evidence gathering for possible criminal offenses. *The Budapest Convention (ETS No. 185) and Its Protocols*, COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/the-budapest-convention [https://perma.cc/WAT9-UH44] (last visited Sept. 21, 2022).

155. *See supra* notes 110-11 and accompanying text.

156. *See Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises*, IDENTITY THEFT RES. CTR. (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ [https://perma.cc/9UHC-KTPF%5d] (reporting that the number of "data compromises" in 2021 was 23 percent over the previous all-time high).

157. For example, Dare2Del is a product that helps "to regulate [] digital knowledge by hiding and deleting irrelevant digital objects such as files or sensor data." *DFG-Project Dare2Del*, GERMAN RSCH. FOUND., https://dare2del.de/ [https://perma.cc/WE87-A7WX] (last updated Nov. 16, 2020). In an associated publication, the research team outlines the methodology of the tool which focused on relational irrelevance — the process of determining when data or files are "irrelevant" in their relation to current high value data, and then proposes to a system administrator to de-list or delete such data based on first order logic. Michael Siebers & Ute Schmid, *Please Delete That! Why Should I?*, 33 KI - KÜNSTLICHE INTELLIGENZ, 2019, at 35, 35-36. This tool is currently equipped for small scale data operations and is illustrative of the potential for more large-scale operation market solutions that can redress the liability balance for organizations holding vast amounts of consumer data..

and to a large scope of personal data will grant consumers a more pronounced measure of control. This Note has argued that if legislators only address deletion standards and avoid the broad exemption of deidentified data alone, then the RTD's potential will be more substantially realized than in its current form.

The Individual as Both Capable and Needy: Internet Access Reimagined Under Martha Nussbaum's Capability Approach to Human Development

Jamie Reiner*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School; B.A., Philosophy, May 2020, Washington University in St. Louis, *cum laude*. Thank you to Ethan Lucarelli, Journal Adjunct, and Julia Heasley, Notes Editor, for their help and encouragment in drafting this Note. And an enduring thank you to Christopher Wellman, for opening my eyes to the magic of philosophical inquiry.

I. INTRODUCTION

"They sit in hot cars, some switching the air conditioning on and off to save fuel. Some just sit on the asphalt using portable TV trays as desks, trying to find shade while staying tethered to the signal."[1] Without reliable Internet access at home, school children like 8-year-old Gabriel Alston struggled to find adequate Wi-Fi to attend remote classes during the throes of the COVID-19 pandemic: "I hate it . . . I can't hear anything on the computer, but when we're in real life, I can hear everyone."[2]

Among the diverse structural deficiencies exposed in the United States through the strain and horror of the COVID-19 crisis, America's lack of reliable and fast Internet access finds itself on the long list. And the numbers support the anecdotes. The Federal Communications Commission ("FCC") approximates that more than 21 million people in the United States do not have reliable Internet connection, and the distribution is not equal.[3] The households without reliable Internet access most often are those that cannot afford it, and thus the children in those homes are left to struggle to find an Internet connection to attend class and complete assignments.[4] This particular manifestation is just one example of how the lack of fast, reliable Internet can hold people back from equal enjoyment, participation, and opportunity in society.

Representative John Lewis encapsulated the current digital chasm in a simple yet prophetic way: ". . . the availability to have access to the Internet . . . is the civil rights issue of the 21st century."[5] How do we understand Internet access? How should our social policies be structured to increase it? What is the proper role of government facilitation? At bottom, this Note seeks to answer those questions through an application of an established theoretical framework to a unique context.

Applying American philosopher Martha Nussbaum's Capability Approach to Internet access would recognize a positive duty on states to secure Internet access as a necessary background condition to providing individuals with the choices and opportunities necessary to decide how to lead their lives. Once accepted, this recognition is helpful for a variety of policy

---

1. Petula Dvorak, *When 'Back to School' Means a Parking Lot and the Hunt for a WiFi Signal*, WASH. POST (Aug. 27, 2020, 4:47 PM), https://www.washingtonpost.com/local/when-back-to-school-means-a-parking-lot-and-the-hunt-for-a-wifi-signal/2020/08/27/0f785d5a-e873-11ea-970a-64c73a1c2392_story.html [https://perma.cc/H2LL-DLXG].

2. *Id.*

3. Joyce Winslow, *Digitally Divided*, 25 TR. MAG., no. 1, Summer 2019, at 26, 28.

4. Emily A. Vogels, *Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption*, PEW RSCH. CTR. (June 22, 2021), https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/ [https://perma.cc/P5Q7-LLE9].

5. The Morning Briefing, *Rep. John Lewis (D-Ga) and Comcast Exec. VP David Cohen Discuss the Internet Essentials Program with Tim Farley*, SIRIUSXM POTUS RADIO, at 02:45 (Aug. 24, 2012), https://soundcloud.com/comcast-1/rep-john-lewis-d-ga-and?utm_source=clipboard&utm_campaign=wtshare&utm_medium=widget&utm_content=https%253A%252F%252Fsoundcloud.com%252Fcomcast-1%252Frep-john-lewis-d-ga-and [https://perma.cc/5ST8-7D76].

questions surrounding attempts to distill what the proper extent of government involvement should be in securing Internet access. Marshalling creativity and innovation from individuals within communities, resulting in broader access, should be the ultimate goal of such policy planning.

Section II lays out four discrete background sections. Subsection A puts forward examples of the deficiencies in the current digital landscape and our increased reliance on Internet access that was amplified by the COVID-19 pandemic, as well as examples of reliance that predated the pandemic. Subsection B explains some of the ways government at the federal, state, and local levels have tried to dampen the digital lacuna. Subsection C explains how the United Nations has taken a human rights approach to the challenge of Internet access rights but argues that this approach does not go far enough towards establishing a positive duty on the State. Lastly, Subsection D lays out the core precepts of Martha Nussbaum's Capability Approach to human development, providing its relevant details and why the nuance matters.

Section III has two sections. Subsection A applies Nussbaum's established theory to the topic of Internet access and suggests that Internet access is required for several of Nussbaum's Central Capabilities. The upshot of this application leads the reader to the conclusion that the government has a positive obligation to promote Internet access. Subsection B then illustrates the consequences of this conclusion by discussing two ways the duty might be implemented by policymakers.

II. BACKGROUND

A. Deficiencies and Reliance: Internet Shortcomings

To appreciate the importance of Internet access, one might start with noting the effects of its absence. The "Homework Gap" and the increase in telehealth use illustrate both the lack of equal access and the need for Internet across all sections of society.[6] Further, beyond the current COVID-19 environment, it is important to appreciate the Internet as a general prerequisite to engaging both in our interpersonal relationships and with our larger political environment.

1. Shortcomings and Reliance Brought on by the Pandemic

The "digital divide" is more than a catchy phrase. It is real, and it manifests itself in a myriad of ways throughout different cross-sections of society.[7] One concerning manifestation is the "Homework Gap" which refers to the lacuna between students who have sufficient Internet access at home and those that do not.[8] The challenges faced by students who lack reliable

6. *See* COLBY LEIGH RACHFAL, CONG. RSCH. SERV., R46613, THE DIGITAL DIVIDE: WHAT IS IT, WHERE IS IT, AND FEDERAL ASSISTANCE PROGRAMS 7 (2021).

7. *Id.*

8. *Id.*

Internet access have been exacerbated in the COVID-19 environment as students are dependent on reliable Internet to attend class and complete their assignments.[9]

During the beginning of the COVID-19 pandemic, 125,000 schools went remote.[10] According to data collected by Pew Research Center's April 2020 survey, "one in five of the surveyed parents said it was at least somewhat likely their children would not be able to complete their schoolwork because they did not have access to a computer at home or would have to use public Wi-Fi to finish their schoolwork."[11] The divide falls on socioeconomic lines as 59% of parents with lower incomes said it's likely their homebound children would face at least one digital obstacle to doing their schoolwork.[12]

The reliance on Internet to continue schooling is just one representation of the strain COVID-19 places on the need for Internet connectivity. The meteoric increase in the use of telehealth represents an additional illustration. As virtual appointments become the new normal for medical care, communities lacking Internet access and digital literacy face steep obstacles to receiving quality care.[13] "Among American adults [over] 65 years old . . . most likely to need chronic disease management, only 55%-60% own a smartphone or have home broadband access."[14] Without reliable Internet access, people are hindered in their ability to go to school and complete our assignments, receive medical care, and even show up for work.[15] In short, those that lack reliable and affordable Internet access often find themselves left behind.

2. General Reliability: Interpersonal and Political Relationships

While the COVID-19 pandemic brought our reliance on Internet access to a critical point, the prominence of the Internet and our dependance on it is not unique to the COVID-19 era. Since its inception, Internet connection has been an integral way to communicate and coordinate our lives with one another. This Note will flesh out two forms of reliance: companionship, the

---

9. *See id.*

10. *Id.*

11. Emily A. Vogels, *59% of U.S. Parents with Lower Incomes Say Their Child May Face Digital Obstacles in Schoolwork*, PEW RSCH. CTR. (Sept. 10, 2020), https://www.pewresearch.org/fact-tank/2020/09/10/59-of-u-s-parents-with-lower-incomes-say-their-child-may-face-digital-obstacles-in-schoolwork/ [https://perma.cc/EWD4-55LU].

12. *Id.*

13. Gezzer Ortega et.al., *Telemedicine, COVID-19, and Disparities: Policy Implications*, 9 HEALTH POL'Y & TECH. 368, 369 (2020).

14. Sarah Nouri et al., *Addressing Equity in Telemedicine for Chronic Disease Management During the Covid-19 Pandemic*, NEJM CATALYST, May 4, 2020, at 1, 2.

15. *See* RACHFAL, *supra* note 6; *see generally* Ashira Prossack, *5 Statistics Employers Need to Know About the Remote Workforce*, FORBES (Feb. 10, 2021, 8:51 PM), https://www.forbes.com/sites/ashiraprossack1/2021/02/10/5-statistics-employers-need-to-know-about-the-remote-workforce/ [https://perma.cc/K8SH-Q8VH] (observing that 74% of the survey volunteers believed that remote work will become the norm even as the pandemic lessens).

way we form and cultivate our relationships with one another; and political involvement, the manner in which we come to learn about our political climate. That is to say, without Internet access, we are unable to fully decide how we foster and grow our social interactions and relationships, nor are we are able to fully participate in the political process.

The advent of the Internet ushered in a new realization: affiliation with one another can transcend physical space.[16] Since the Internet's proliferation, relationships have been created, fostered, and endured online as "the Internet provides the means for inexpensive and convenient communication . . . it increases communication among friends and family, especially contact with those who are far away."[17] A ripe example can be seen through the trend in finding one's life partner through Internet platforms.[18] According to one study from Stanford University, "Internet meeting is displacing the roles that family and friends once played in bringing couples together."[19] The study found that there has been a consistent increase in romantic relationships beginning online, and the trend only continues to increase as technology and smartphone use maintains a dominant presence in our lives.[20] Further data supports what, in retrospect, seems patently obvious:

> Internet use provides online Americans a path to resources, such as access to people who may have the right information to help deal with a health or medical issue or to confront a financial issue . . . . The result is that people not only socialize online, but they also incorporate the Internet into seeking information, exchanging advice, and making decisions.[21]

Internet access has replaced our physical communities as the nexus for communication and personal connection. Without the Internet, we are stymied in the quantity, quality and richness of the relationships we are capable of having with one another. Without reliable Internet access, we are limited in the communities we are able to create and the people that we may meet.

A further facet of our reliance on Internet access comes in the form of political participation. Widespread use of technology is now how we get information about our elected officials, leading to a more informed

16. JEFFREY BOASE ET AL., PEW INTERNET & AM. LIFE PROJECT, THE STRENGTH OF INTERNET TIES, at ii (2006), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2006/PIP_Internet_ties.pdf.pdf [https://perma.cc/9V4D-CCB3].

17. Barry Wellman, et al., *The Social Affordances of the Internet for Networked Individualism*, 8 J. COMPUT.-MEDIATED COMM. 1 JCMC834 (2003); *see also* BOASE ET AL., *supra* note 16, at 10 (noting the prominence of Internet in everyday life).

18. Michael J. Rosenfeld et al., *Disintermediating Your Friends: How Online Dating in the United States Displaces Other Ways of Meeting*, 116 PNAS 17753, 17753 (2019).

19. *Id.*

20. *Id.* at 17756.

21. BOASE ET AL., *supra* note 16, at 10.

citizenry.[22] Because the Internet not only provides a platform for voters to receive information, but also a way for candidates to communicate with voters, political engagement is increasingly occurring online.[23] Without reliable Internet access, informed citizenship is strained, and political involvement dampened.

Beyond social media's use for engagement in elections, it also facilitates social movements.[24] Social media is a tool to streamline organization, as well as a platform to express discontent with the status quo.[25] Approximately 23 percent of adults that use social media note that their views on a political or social issue have changed as a result of being tuned into the digital political discourse.[26] Lastly, democratic engagement set aside, social media, and Internet access more generally, has and continues to play a central role in political reformation across the world.[27]

B. Government Recognition of Internet Shortcomings and Import

Despite the contemporary necessity of and reliance on Internet access articulated above, the United States continues to fall short in providing accessible and affordable Internet access. While government, at all levels, has not been silent on this issue, persistent inequality endures.[28]

Action taken by the federal government to reach further equity often takes the form of broad, top-down funding schemes, while courses of action taken by local and state governments tend to utilize creative, innovative methods to further broadband access.[29] This section takes a non-exhaustive look at the policies currently in place and the various obstacles faced.

---

22. *See* JANNA ANDERSON & LEE RAINIE, PEW RSCH. CTR., MANY TECH EXPERTS SAY DIGITAL DISRUPTION WILL HURT DEMOCRACY 92 (2020), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/02/PI_2020.02.21_future-democracy_REPORT.pdf [https://perma.cc/MX5D-QQVN].

23. PEW RSCH. CTR., CHARTING CONGRESS ON SOCIAL MEDIA IN THE 2016 AND 2020 ELECTIONS 4 (2021), https://www.pewresearch.org/politics/wp-content/uploads/sites/4/2021/09/PDL_09.30.21_congress.twitter.final_.pdf. [https://perma.cc/RE2B-3X6X].

24. Brooke Auxier, *Social Media Continue to Be Important Political Outlets for Black Americans*, PEW RSCH. CTR. (Dec. 11, 2020), https://www.pewresearch.org/fact-tank/2020/12/11/social-media-continue-to-be-important-political-outlets-for-black-americans/ [https://perma.cc/Q37P-W664] (finding that, especially for Black Americans in the wake of police brutality, social media has provided outlets to connect with one another and gain information on protests and political activism generally).

25. Andrew Perrin, *23% of Users in U.S. Say Social Media Led Them to Change Views on an Issue; Some Cite Black Lives Matter*, PEW RSCH. CTR. (Oct. 15, 2020), https://www.pewresearch.org/fact-tank/2020/10/15/23-of-users-in-us-say-social-media-led-them-to-change-views-on-issue-some-cite-black-lives-matter/ [https://perma.cc/74LX-NV62].

26. *See id.*

27. *See* Noureddine Miladi, *Social Media and Social Change*, 25 DIG. MIDDLE E. STUD. 36, 38 (2016) (noting the role of Twitter in Egyptian and Tunisian revolutions).

28. *See* Vogels, *supra* note 4.

29. *See* discussion *infra* p. 354.

1. Federal Action

Most recently, the Infrastructure Investment and Jobs Act, passed in 2021, allocates significant resources to broadband buildout.[30] Specifically, the legislation apportioned $42.45 billion to the states to be used for broadband programs.[31] Further, $14.2 billion is allocated to subsidize the cost for low-income households.[32] This funding scheme demonstrates a financial commitment toward lessening digital inequity in the United States. Beyond the new infrastructure scheme, in January 2020, the FCC implemented the Rural Digital Opportunity Fund that works to expand broadband access to rural communities.[33] Specifically, this program allocates $20.4 billion over the course of ten years "to fund the deployment of high-speed broadband networks in rural America."[34]

2. Community Gap Filling: Furthering Access Through Creativity

Setting aside the federal programs discussed above, the focus below is to highlight distinctive and creative ways that government action at the local and state level tries to fill the gaps in access left unfilled by the private-sector.[35] That is to say, while the federal government has taken cognizable steps in furthering Internet access, the federal programs have been largely removed from on-the-ground community needs. This section focuses on two resourceful ways communities have tried to further broadband access: municipal broadband and federal asset deployment.

Municipal broadband, also known as community broadband, is an inventive way through which various communities throughout the United States, often underserved and lacking accessible and/or affordable broadband, have taken matters into their own hands.[36] The ultimate goal is to both

30. *See* Margaret Harding McGill, *Infrastructure Bill Includes Billions for Broadband*, AXIOS (Nov. 8, 2021), https://www.axios.com/infrastructure-bill-broadband-911dea37-b38d-4f33-901e-ec6eb73650c4.html [https://perma.cc/LPT2-VG2D].

31. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 60102(b)(2), 135 Stat. 429, 1184 (2021).

32. § 60502, 135 Stat. at 1238, 1382.

33. *Auction 904: Rural Digital Opportunity Fund*, FCC, https://www.fcc.gov/auction/904 [https://perma.cc/SL2T-HMX8].

34. COLBY LEIGH RACHFAL, CONG. RSCH. SERV., R46307, STATE BROADBAND INITIATIVES: SELECTED STATE AND LOCAL APPROACHES AS POTENTIAL MODELS FOR FEDERAL INITIATIVES TO ADDRESS THE DIGITAL DIVIDE 3 (2020).

35. These varied programs and initiatives often take the form of broad, top-down policy plans necessarily removed from the on-the-ground needs in communities underserved or even sometimes forgotten by private Internet service providers ("ISPs"). *See* discussion *infra* p. 355.

36. *See* LENNARD G. KRUGER & ANGELE A. GILROY, CONG. RSCH. SERV., R44080, MUNICIPAL BROADBAND: BACKGROUND AND POLICY DEBATE 1 (2016).

increase the number of people that have access to broadband and provide the service at a low cost.[37]

Municipal broadband is distinct from the traditional way most Americans receive their Internet access.[38] Broadband, used interchangeably with the term "high-speed Internet," is most often provided by private sector telecommunication companies (e.g., Verizon, Comcast).[39] This typical broadband structure is effective in providing reliable Internet access to cities and metropolitan suburbs.[40] But these companies often overlook more rural areas.[41] Municipal broadband can improve upon the deficiencies of private market companies.[42] Communities underserved by private-sector Internet Service Providers ("ISPs") often find themselves disappointed in their lack of broadband access or if they do receive broadband, in the quality of their connection.[43] As of 2015, approximately 500 communities were implementing some type of municipal broadband by building (and in some cases operating) their own publicly-financed broadband infrastructure.[44] Municipal broadband programs take varied forms because "[p]ublic entities that provide broadband service can be local governments or public utilities . . . . [s]ince each community is different and faces unique challenges, there is no one size that fits all."[45]

Lafayette, Louisiana is an example. In 2005, the citizens of Lafayette voted to build a municipal fiber network.[46] This network ushered in lower prices, furthered access, and brought jobs into the community.[47] It also had trickle-down effects that extended beyond the scope of broadband. Because the speed was so fast—100Mb/s down—and because the rates were affordable, the project led companies to create office locations in Lafayette.[48] As this example illustrates, the most obvious advantage of municipal broadband is what it enables smaller communities to accomplish: faster download and upload speeds.[49] It also serves the function of injecting

37. *See Our Vision*, CMTY. BROADBAND NETWORKS, https://muninetworks.org/content/our-vision [https://perma.cc/89BL-2MJD] (last visited Mar. 15, 2023).
38. *See* KRUGER & GILROY, *supra* note 36, at 1.
39. *See id.*
40. *See id.*
41. *See id.*
42. *See id.*
43. *See id.*
44. *See* KRUGER & GILROY, *supra* note 36, at 1.
45. *See id.*
46. *Id.* at 5.
47. *See id.*
48. *See id.*
49. *See id.* at 3.

competition into markets where it often is scant.[50] Competition in the market is important, as it serves to keep costs low and quality high.[51]

Although municipal broadband tends to be championed by the communities it serves, it is a contested policy, and its lifespan remains threatened by many state legislatures.[52] For example, nineteen states have passed laws or otherwise placed restrictions on the creation of local municipal networks.[53] The success of municipal broadband rises and falls with the state legislatures because local governments are considered "political subdivisions of a state" and therefore do not have any independent authority to act "absent a delegation of such power from a state."[54]

The upshot is that if a state legislature decides against municipal broadband, it can pass a state law that prevents municipalities from implementing their own broadband schemes.[55] States may hesitate to allow municipal broadband to flourish for several reasons.[56] One concern is that it is "inappropriate" for government-funded networks to compete with private providers.[57] Other reasons proffered look to the complicated deployment of broadband and the insistence that taxpayer funds should be spent on basic needs that traditionally fall under the government's domain such as bridges and roads.[58]

Faced with pushback from states, municipalities have approached the FCC "to preempt state laws that restrict municipal participation in broadband or telecommunications."[59] In 1987, a Missouri law prevented municipalities from providing telecommunications services.[60] Subsequently, the municipalities petitioned the FCC to preempt the state law under Section 253 of the Communications Act of 1934, which gave the FCC the power to preempt state or local laws that "may prohibit or have the effect of prohibiting the ability of any entity to provide"[61] telecommunications services.[62] But the FCC declined to intervene because "the term 'any entity' in section 253(a) . . . was not intended to include political subdivisions of the state, but

50. *See* KRUGER & GILROY, *supra* note 36, at 4.

51. EXEC. OFF. OF THE PRESIDENT, COMMUNITY-BASED BROADBAND SOLUTIONS: THE BENEFITS OF COMPETITION AND CHOICE FOR COMMUNITY DEVELOPMENT AND HIGHSPEED INTERNET ACCESS 11 (2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/community-based_broadband_report_by_executive_office_of_the_president.pdf [https://perma.cc/9N4Z-5BNN].

52. *See id.* at 13.

53. *See id.* at 4.

54. CHRIS D. LINEBAUGH & ERIC N. HOLMES, CONG. RSCH. SERV., R46736, STEPPING IN: THE FCC'S AUTHORITY TO PREEMPT STATES LAWS UNDER THE COMMUNICATIONS ACT 34 (2021).

55. Tyler Cooper, *Municipal Broadband 2022: Barriers Remain an Issue in 17 States*, BROADBANDNOW (Oct. 23, 2022), https://broadbandnow.com/report/municipal-broadband-roadblocks/ [https://perma.cc/6D3G-D9JG].

56. *See* KRUGER & GILROY, *supra* note 36, at 4.

57. *See id.*

58. *See id.*

59. LINEBAUGH & HOLMES, *supra* note 54, at 31.

60. MO. REV. STAT. § 392.410 (2016).

61. *See* 47 U.S.C. § 253(a); *see also* LINEBAUGH & HOLMES, *supra* note 54, at 31-32.

62. *See* 47 U.S.C. § 253(a).

rather appears to prohibit restrictions on market entry that apply to independent entities subject to state regulation."[63] The dispute rose through the courts in *Nixon v. Missouri Municipal League.*[64]

Nixon eventually reached the United States Supreme Court, where the Court agreed with the FCC.[65] Justice Souter argued that the "working assumption that federal legislation threatening to trench on the States' arrangements for conducting their own governments should be treated with great skepticism."[66] Without a clear delegation of power given from Congress to the FCC, the Commission lacked clear authorization to preempt state laws.[67]

After *Nixon* came *Tennessee v. FCC,* which furthered the preemption debate.[68] The cities of Wilson, North Carolina and Chattanooga, Tennessee "sought to expand coverage of their broadband networks beyond what state law would permit and asked the FCC to preempt their respective state's law to allow expansion."[69] This time, the FCC stepped in, relying on Section 706 of the Communications Act of 1934, which states: "the Commission . . . shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity . . . or other regulating methods that remove barriers to infrastructure investment."[70]

While the text of § 706 does not expressly give the FCC preemption power, the FCC considered preemption to be encapsulated by the words "regulate and remove barriers."[71] The Sixth Circuit rejected the FCC's interpretation and overturned its preemption, citing that the state's decision, akin to *Nixon* "implicate[d] core attributes of state sovereignty . . . "[72] These cases make clear that the FCC is currently limited in its ability to preempt state laws that prevent community broadband without Congress first issuing a plain statement to the FCC.[73]

A constitutional question still lingers: because the Supreme Court and the Sixth Circuit rested their holdings on the fact that Congress had not issued a "plain statement," it remains a Constitutional question "whether Congress could, consistent with the Constitution, provide the FCC with the power to preempt state laws regulating municipal broadband."[74] Although there is no

---

63. Mo. Mun. League, *Memorandum Opinion and Order*, 16 FCC Rcd 1157, para. 9 (2001), *vacated sub nom.* Mo. Mun. League v. FCC, 299 F.3d 949 (8th Cir. 2002), *rev'd sub nom.* Nixon v. Mo. Mun. League, 541 U.S. 125 (2004); *see* LINEBAUGH & HOLMES, *supra* note 53, at 33 (noting that this issue arises because Congress has not issued a "plain statement" delegating pre-emption power to the FCC).

64. *See Nixon*, 541 U.S. at 140-41.

65. *See id.* at 140-41.

66. *See id.* at 140.

67. *See id.* at 140-41 (citing Gregory v. Ashcroft, 501 U.S 452, 495 (1991)).

68. *See* Tennessee v. FCC, 832 F.3d 597 (6th Cir. 2016).

69. LINEBAUGH & HOLMES, *supra* note 54, at 5.

70. *See* 47 U.S.C. § 1302.

71. *See id.*; *see also* LINEBAUGH & HOLMES, *supra* note 54, at 32.

72. *Tennessee*, 832 F.3d at 611-12.

73. LINEBAUGH & HOLMES, *supra* note 54, at 32.

74. *See id.* at 33.

clear answer, precedent suggests that such an authorization would be constitutionally permissible.[75]

Beyond municipal broadband, another creative approach to furthering broadband buildout is to use existing infrastructure.[76] This includes assets such as "tower facilities, buildings, and land . . ."[77] Private companies can obtain federal permits to use these assets, which facilitate easier broadband buildout.[78] These permits provide private companies that struggle reaching rural communities with infrastructure needed for broadband buildout, furthering the ultimate goal of providing access to more people.[79] Eliminating the obstacle of insufficient infrastructure is one way access can be furthered.[80]

Importantly, marshaling these assets requires fostering a relationship between private-sector companies and federal agencies such as the Department of Interior and the Department of Homeland Security in order "to streamline the federal permitting process and make it easier for network builders to access federal assets and rights-of-way."[81] The ultimate goal is to open up existing federal assets through a permitting process, which would ultimately decrease the cost of furthering broadband access and encourage private companies to broaden their deployment.[82]

Action taken by Arizona Governor Doug Ducey provides a helpful illustration of this idea. In January 2020, Governor Ducey announced that almost $50 million in funding would be given to the Arizona Department of Transportation to install "more than 500 miles of broadband conduit and fiber optic cable along designated highway segments in rural areas of the state."[83] Here, the pre-existing highway will be used as a means to further deploy broadband to more rural communities.[84] Through this action, broadband will reach remote communities often left behind by traditional Internet planning schemes.

The above section detailed a variety of governmental actions undertaken to curtail digital inequity. Yet, a lacuna still remains. From a conceptual standpoint, the United States has stopped short of understanding and actualizing Internet access as a human right, a theory that has been endorsed by the United Nations.[85]

---

75. *See* Lawrence Cnty. v. Lead-Deadwood Sch. Dist., 469 U.S. 256, 270 (1985) (finding that a federal statute authorizing a local government to spend federal funds preempted state law requiring funds to be spent in a particular manner).
76. RACHFAL, *supra* note 34, at 7.
77. *See id.* at 8.
78. *See id.*
79. *See id.*
80. *See id.* at 7.
81. *See id.* at 8.
82. *See* RACHFAL, *supra* note 34, at 8.
83. *See id.*
84. *See id.*
85. *See* discussion *infra* p. 359.

C. Internet Access as a Human Right: The Approach of the United Nations

Although the United States has stopped short of defining Internet access as a human right, the United Nations ("UN") has embraced the categorization.[86] Created in the shadow of WWII, the UDHR is a document treated as the standard for the codification and protection of fundamental human rights and is understood as a cross-border standard "for all peoples and all nations."[87]

The UDHR is a collective check on governmental power, as it specifies rights that should be protected cross-culturally.[88] Specifically, Article 19 states that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[89] In 2016, based on Article 19, Section 2 of the International Convention on Civil and Political Rights, the UN issued a non-binding resolution stating that all persons have a right to Internet access.[90] The thirty-second session of the Human Rights Council, titled "The Promotion, Protection, and Enjoyment of Human Rights on the Internet" further detailed the right to freedom of expression on the Internet.[91]

Although the UDHR is not binding, it serves as a foundational, guiding document in the drafting of "many national constitutions and domestic legal frameworks."[92] Important for the present discussion, the UN's non-binding resolution is couched in terms of negative liberty.[93] Governments should not block or limit Internet access.[94] Negative liberty importantly stops at interference. It does not work to promote Internet access, but rather, it addresses actions taken by government in restricting access. This Note argues that understanding government responsibilities in the negative—that is, through a non-interference lens—does not go far enough in actualizing human rights.

There has been substantial debate within the scholarly discourse, and among rights theorists more generally, about whether states have a positive

---

86. *See generally* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948); Human Rights Council Res. 32/L.20, U.N. Doc. A/HRC/RES/32/L.20, at 2 (June 27, 2016).

87. *See generally* G.A. Res. 217 (III) A, Universal Declaration of Human Rights; *see* Catherine Howell & Darrell M. West, *The Internet as a Human Right*, BROOKINGS (Nov. 7, 2016), https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ [https://perma.cc/2U8V-GLHT].

88. *See generally* G.A. Res. 217 (III) A, *supra* note 84.

89. *See id.* at Art. 19.

90. Human Rights Council Res. 32/L.20, U.N. Doc. A/HRC/RES/32/L.20, at 2.

91. *See id.* at 2.

92. *Universal Declaration of Human Rights*, AMNESTY INT'L, https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/ [https://perma.cc/LYN9-ZGT4] (last visited Mar. 15, 2023).

93. *Id.*

94. *See* Howell &West, *supra* note 87.

duty to promote (or even provide) Internet.[95] The biggest concern is placing a technology at the same level of importance as uncontroverted human rights such as the freedom of movement or expression.[96] Can something that is less than forty years old be equated with the most fundamental and essential rights of individuals?[97] Does this imply that human life lacks meaning without reliable and fast Internet access?[98] Should we be concerned with elevating technology to such a high status?[99] Martha Nussbaum's adaptation of Capability Theory provides a framework for addressing the concern behind these theoretical questions.

D. Martha Nussbaum's Capability Theory

This section will introduce Martha Nussbaum's Capability Theory. It represents a human-centered approach to public and social policy planning which, when applied to the issue of Internet access, allows for a re-understanding of government involvement in securing broadband access.

1. Introduction to Capability Theory

Broadly speaking, Nussbaum's Capability Approach to human development is a conceptual framework used in the fields of human development, moral philosophy, and human rights.[100] Capability Theory (hereinafter used interchangeably with the term "Capability Approach") is first and foremost a theory of human development and justice.[101] It is a global theory that argues for a floor, not a ceiling, in asking what the basic, non-arguable requirements that all human beings need in order to live a truly human life.[102] Put differently: What are the basic threshold requirements that allow people to "function well"?[103] At bottom, Nussbaum's flavor of

95. *See* Brian Skepys, *Is There a Human Right to the Internet?*, 5 J. POL. & L., no. 4, 2012, at 15, 15 (arguing that Internet should not be considered a human right because it is not a prerequisite for membership in a political community, but rather its absence can be understood as a "potentially urgent threat to a more basic list of human rights"); *see also* Jonathan W. Penney, *Internet Access Rights: A Brief History and Intellectual Origins*, 38 MITCHELL L. REV. 10, 17 (2011) (noting one strain of Internet rights advocates focus on the new advent of the cyberspace and the need to be able to connect with one another); Vinton G. Cerf, *Internet Access Is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html [https://perma.cc/BTU6-7LXZ] (arguing that Internet access is valuable as a means, rather than an end that is independently valuable).

96. *See* Cerf, *supra* note 95.

97. *See id.*

98. *See id.*

99. *See id.* (noting one cause for concern is technology's ever-evolving nature, which raises the question: does each subsequent technology get added to the list of basic human rights?).

100. *See* Chad Kleist, *Global Ethics: Capabilities Approach*, INTERNET ENCYC. OF PHIL., https://iep.utm.edu/ge-capab/#H3 [https://perma.cc/T59F-R66U] (last visited Sept. 27, 2022).

101. *See id.*

102. *See id.*

103. Martha C. Nussbaum, *Human Functioning and Social Justice: In Defense of Aristotelian Essentialism*, 20 POL. THEORY 202, 214 (1992).

Capability Theory begins by asking a simple question: "What are people actually able to do and be?"[104]

By premising her theory on a value-laden question, Nussbaum presupposes " . . . a certain conception of 'the good life.'"[105] In articulating her list of the Ten Central Capabilities (detailed below), without which one's basic human needs are not being met, Nussbaum's articulation of the good life is one of "human flourishing," one that is engaged in a normative evaluation.[106] Nussbaum contends that her list of Ten Central Capabilities represents a "thick but vague conception of the good."[107] It is "thick" because her analysis originates from and is targeted to a central, value laden question: What do people need to be able to do, regardless of what community they belong to?[108] By asking that question, and further, by centering her entire theory around that question, she outlines an ideal (although minimalistic and basic) of what a truly "human" life looks like.[109] The Ten Central Capabilities consider human beings both "capable and needy."[110]

Ten Central Capabilities[111]

1. Life
2. Bodily health
3. Bodily Integrity
4. Senses, imagination, and thought
5. Emotions
6. Practical reason
7. Affiliation
    a. Friendship
    b. Respect
8. Other species
9. Play
10. Control Over One's Environment
    a. Political
    b. Material

Describing each of Nussbaum's Central Capabilities is not needed to understand the thrust of her argument. However, because they are relevant for the application section below, two capabilities will be explained: "Affiliation," specifically "Friendship," and "Control Over One's Environment," specifically "Political."

---

104. *See id.*

105. Kleist, *supra* note 100.

106. *See id.* (noting that Nussbaum's "'thick' but 'vague'" theory is conceptually different from other theories); *see also* Nussbaum, *supra* note 103, at 214-15 (distinguishing her "thick vague theory of the good" from John Rawls' "thin theory of the good," which is a theory of justice focusing on what is needed by anyone living out any conception of the good).

107. Kleist, *supra* note 100.

108. *Id.*

109. Nussbaum, *supra* note 103, at 220.

110. *Id.* at 216, 220.

111. *See* Martha C. Nussbaum, *Capabilities and Human Rights*, 66 FORDHAM L. REV. 273, 287-88 (1997).

Nussbaum defines "Friendship" as "being able to live for and to others, to recognize and show concern for other human beings, to engage in various forms of social interaction; to be able to imagine the situation of another and to have compassion for that situation; to have the capability for both justice and friendship."[112] Nussbaum defines "Control Over One's Environment," specifically one's "Political" environment, as: "being able to participate effectively in political choices that govern one's life; having the right of political participation, protections of free speech and association."[113]

Nussbaum is clear: "all the central capabilities, like all human rights, are best seen as occasions for choice, areas of freedom . . ."[114] The capabilities on this list constitute Combined Capabilities.[115] Combined Capabilities require both "the internal preparation for action and choice, plus circumstances that make it possible to exercise that function."[116] For instance, "the capability of free speech requires not only the ability to speak," (internal capability),"but also the actual political and material circumstances" that make it possible to exercise that function.[117]

The Combined Capabilities are necessarily pre-political, meaning they attach to human beings "independently of and prior to membership in a state."[118] Importantly, when the ideas are combined, "the ten capabilities then are *goals* that fulfill or correspond to people's pre-political entitlements . . . . In the context of a nation, then it becomes the job of government to secure them . . . ."[119]

The policy implications of Nussbaum's list of Central Capabilities are that government planning should be focused around setting up every person to be able to decide if they want to actualize their capabilities. At bottom, the connection between these ten capabilities dictates the focus of government planning.

2. Capabilities, Not Functions: On Their Difference and Why it Matters

Before moving on to further discussion of capabilities, it is important to understand the difference between capabilities and functions. This section explains the relationship between capabilities and functions and how capability—that is, the choice structure to actualize the function—represents the heart of Nussbaum's theory.[120] A comparative discussion of capabilities and functions helps to distill the subtle difference between the two levels of abstraction.

---

112. *Id.* at 287.
113. *Id.* at 288.
114. Martha C. Nussbaum, *Capabilities, Entitlements, Rights: Supplementation and Critique*, 12 J. HUM. DEV. & CAPABILITIES 23, 28 (2011).
115. *Id.* at 25.
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. *See* Nussbaum, *supra* note 112, at 277-78.

Nussbaum's account requires appreciating the conceptual difference between capabilities (ten of which are listed above as part of Nussbaum's Central Capability List) and functions. Nussbaum is clear: "capability, not functioning, is the political goal."[121] The distinction is key because it strikes to the very heart of the theory's framework. Functions are undertakings that individuals can pursue, such as education, traveling, and getting married.[122] Capabilities "are the real, or substantive, opportunit[ies] that they have to achieve . . ." their specific functions, such as access to schooling, public infrastructure and civil institutions (for marriage).[123] Capabilities necessarily come prior to functions.

An illustrative example helps capture the distinction between a capability and a function: the difference between fasting and starving.[124] The difference between not eating because one decides to fast versus not eating because there is no available food is the difference between a function and capability.[125] An individual does not *have* to eat (the opportunity or choice structure here is the function), but an individual needs to have the ability or capability to give their body nutrients.[126] Opportunity (function) is premised on the existence of capabilities because "[a] capability . . . is simply the freedom that people have to do or be certain things."[127]

The ultimate goal for the government is one that secures capabilities, not functions, because in a free society, it is up to each individual to decide how much to eat and work, what to do, how to think, and what to feel and believe.[128] Securing capabilities gives the individual the building blocks, or the choice structure, to decide how to lead their lives.[129] At bottom, capabilities are worried about securing for each individual "the opportunity to choose."[130]

3. Tripartite Form of Capabilities

There are three different kinds of capabilities under Nussbaum's framework.[131] The first, most elemental type of capability is denoted as a basic capability.[132] A basic capability is understood as "the innate equipment of individuals that is the necessary basis for developing the more advanced capability."[133] Nussbaum provides the example of infants: "most infants have

121. *See id*. at 289.
122. *See id.* at 288.
123. Ingrid Robeyns & Morten Fibieger Byskov, *The Capability Approach*, STAN. ENCYC. OF PHIL. ARCHIVE, https://plato.stanford.edu/archives/win2021/entries/capability-approach/ [https://perma.cc/8ACS-UPLA] (last updated Dec. 10, 2020).
124. Nussbaum, *supra* note 112, at 289.
125. *See id.*
126. *See id.*
127. Robeyns & Byskov, *supra* note 124.
128. Nussbaum, *supra* note 112, at 289.
129. *See id.*
130. *See id.*
131. *See id.*
132. *See id.*
133. *See id.*

from birth the *basic capability* for practical reason and imagination . . ."[134] Infants possess these basic capabilities even though they are unable to fully use these capabilities until they are older and "have a lot more development and education."[135] Basic capabilities are the essential building blocks that can be further actualized as more life experience is gained.[136]

Second, internal capabilities focus on the individual self and look at "states of the person herself that are, so far as the person herself is concerned, sufficient conditions for the exercise of the requisite function."[137] A clarifying example: most adult human beings have "the internal capability to use speech and thought in accordance with their own conscience." [138] Internal capabilities are, by definition, inwardly focused.[139] They capture the manner in which the individual is positioned to actualize functions if they choose.[140]

Third are combined capabilities, which are defined as "internal capabilities *combined with* suitable external conditions for the exercise of the function."[141] To secure combined capabilities, the internal capability of an individual needs to be met with the relevant environmental and political circumstances that allow the capability to actually mean something.[142] An example of the way a combined capability operates: "citizens of repressive non-democratic regimes have the internal but not the combined capability to exercise thought and speech in accordance with their conscience."[143]

Nussbaum asserts that "the aim of public policy is the production of Combined Capabilities."[144] That is to say, the state has the duty to ensure that individuals have both the internal and external factors to be able to perform the functions of the Central Capabilities.[145] To be considered a free state, citizens must be able to decide how to lead their lives.[146] By setting Combined Capabilities as a governmental goal, the focus is placed on creating the opportunities for people to decide how to lead their free and autonomous lives.[147] Internal capabilities are promoted "by providing the necessary education and care" and the external capabilities are promoted through external conditions that allow functions to occur.[148] Although internal capabilities are necessarily directed toward functioning, as stated above, the goal of this theory is to put individuals in a position to be able to actualize those functions if they *choose*; it is not coercive.[149] The ultimate goal is to

134. Nussbaum, *supra* note 112, at 289.
135. *See id*.
136. *See id*.
137. *See id.*
138. *See id.*
139. *See id.* at 290.
140. Nussbaum, *supra* note 112, at 290.
141. *See id.* at 289-90.
142. *See id.* at 290.
143. *See id.*
144. *See id.*
145. *See id.*
146. Nussbaum, *supra* note 112, at 289.
147. *See id.*
148. *See id*.
149. *See id.*

promote internal and external factors so that if an individual wants to exercise certain functions, such as practical reason, they are positioned to successfully actualize their desires.[150] Nussbaum makes clear: "I am not pushing individuals into the function: once the stage is fully set, the choice is up to them."[151]

While the state lacks the ability to control internal factors, under Nussbaum's theory, the state has the power to create the relevant external factors that are needed.[152] The focus of state policymaking should therefore be on the external, material background conditions that the state has the ability to promote.

Once the basic contours of the Capability Approach are understood, the theory illustrates a larger point: "what is involved in securing a right to people is usually a lot more than simply putting it down on paper."[153] The theory is creative because it is able to cut through traditional rights discourse as, "the right to political participation, the right to religious free exercise . . . are all best thought of as human capacities . . . to function in certain ways.[154] Importantly, Nussbaum's theory highlights the interdependence between the two component parts (internal capabilities as well as external conditions of the environment) and illustrates that possessing one and not the other is insufficient as "a citizen who is systematically deprived of information about religion does not really have religious liberty, even if the state imposes no barrier to religious choice."[155] Having the internal capability but lacking the necessary external conditions also comes up short.[156]

The language of capabilities underscores the importance of being able to actually *act* on the choices you have.[157] If securing background conditions is the ultimate goal, states must do more than simply not block individuals from acting.[158] Ultimately, negative liberty will be insufficient.[159]

III. ANALYSIS

Applying Nussbaum's Capability framework to Internet access illuminates its importance and the corresponding government responsibility in two main ways. First, Nussbaum's approach sidesteps common theoretical obstacles that rights theorists often face when engaging in human rights

150. *See id.* at 290.
151. *See id.*
152. *See* Nussbaum, *supra* note 112, at 291.
153. *See id.* at 293.
154. *See id*.
155. See *id.*
156. *See id.*
157. *See id.*
158. *See* Martha C. Nussbaum, *Human Rights and Human Capabilities*, 20 HARV. HUM. RTS. J. 21, 22 (2007).
159. Polly Vizard, et al., *Introduction: The Capability Approach and Human Rights*, 12 J. HUM. DEV. & CAPABILITIES 1, 2-4 (2011).

discourse.[160] Instead of starting with struggling to define what constitutes a human right and then working to shoehorn an understanding of Internet access into an existing framework, Nussbaum's Capability Approach looks to what background conditions are required in order for people to decide how to lead their lives.[161] The conversation can pivot away from a rights-centric discussion and take a less radical, more functional approach that looks to determine what individuals, both *capable and needy*, require to lead autonomous lives.[162] Under Nussbaum's framework, Internet access is the necessary external component.[163] It is the linchpin to securing many of the Central Capabilities.

Second, adopting the framework has real-time policy consequences. Once accepted, Nussbaum's framework makes clear that government has a positive duty to facilitate widescale broadband access. The upshot of this suggests that there should be a greater degree of government involvement in reducing obstacles to furthering digital equity.

A. Application

Without substantive efforts to provide reliable Internet access, the United States government fails to provide the "material institutional environment" needed to secure several of the Central Capabilities on Nussbaum's list.[164] Internet access is a necessary background condition needed to actualize many of Nussbaum's Central Capabilities. This section will focus on two of Nussbaum's Central Capabilities: "Affiliation," specifically "Friendship," and "Control Over One's Environment," specifically "Political."[165] By showing how Internet access is needed for these Central Capabilities to exist, the case for Internet access as a necessary material condition is established, thus placing a positive duty on governments.

For the vast majority of individuals in the U.S., our affiliations, and more generally, our companionships, have evolved and now require the background condition of Internet access. As discussed above, Nussbaum defines friendship as the ability to "live for and to others, to recognize and show concern for other human beings, to engage in various forms of social interaction . . ."[166] Having the capability, and, thus, the associated choice structure, requires "protecting institutions that constitute such forms of affiliation."[167] Without Internet access, social interaction generally and friendship specifically are diminished. When we seek engagement, be it with friends or strangers, we connect over the Internet. Social media platforms

160. *See* Cerf, *supra* note 95 (noting the concern of classifying a technology as a human right). Nussbaum's Capability framework is able to avoid a conceptually challenging conversation of weighing the advantages and disadvantages of classifying a technology as a human right.

161. *See id.*

162. *See id.*; Nussbaum, *supra* note 103, at 216, 220.

163. *See* Nussbaum, *supra* note 112, at 293.

164. *See* Nussbaum, *supra* note 115, at 23, 31-32.

165. Nussbaum, *supra* note 112, at 288.

166. *See id.* at 287-88.

167. *See id.* at 287.

have usurped the traditional roles of in-person meet-ups and town hall discussions.[168] Not only is social media where we connect with those that we know; social media also has the power to connect strangers seeking human connection.[169]

Second, having control over one's political environment now requires Internet access. The Internet is needed to secure background conditions of engaging in the political process, as most political engagement occurs online. Without reliable Internet access, one's ability to research, interact, and learn political information is materially dampened. In one study conducted by Pew Research Center, about half of the people who use social media between the ages of eighteen to twenty-nine explained that they use social media to gain information about political rallies and gatherings.[170] A lack of digital equity creates divergences in political education and involvement. Those who have Internet access are able to engage in the broader community and are thus able to be part of larger social and political networks.[171] Those that do not have access are left out. Even beyond domestic social movements, Internet access broadly and social media generally has played integral roles in political revolutions, such as in Tahrir Square in 2011.[172] For example, social media played a critical role in the Egyptian revolution.[173] The environment it created enhanced peaceful political and human rights activism as opposed to violent protests."[174]

Internet access is part of the external environment and, therefore, is part of the specific circumstances needed for both the capability to affiliate with others and to engage in political discourse. Without reliable Internet access existing in the background, internal abilities, while possessed, cannot be meaningfully realized.[175] Nussbaum's framework sheds light on what might seem obvious but has not yet been considered: the negative duty proclaimed by the UN is not enough—there is a positive obligation to actively promote and spread its accessibility and affordability.

---

168. *See* Packingham v. North Carolina*,* 137 S. Ct. 1730, 1737 (2017) (holding that the Internet has now become "the modern public square" and restricting access to certain websites was in violation of an individual's First Amendment rights); *see also* Knight First Amend. Inst. at Colum. Univ. v. Trump, 928 F.3d 226, 236 (2d Cir. 2019) (finding that while Donald Trump was serving as a government employee, Donald Trump's Twitter account constituted a public forum).

169. Amber D. DeJohn et al., *Identifying and Understanding Communities Using Twitter to Connect About Depression: Cross-Sectional Study*, 5 J. JMIR MENTAL HEALTH, no. 4, 2018, 1, 8 (finding that people who suffer from depression are increasingly looking to social networking platforms, especially Twitter, for support systems).

170. Brooke Auxier, *Activism on Social Media Varies by Race and Ethnicity, Age, Political Party*, PEW RSCH. CTR. (July 13, 2020), https://www.pewresearch.org/fact-tank/2020/07/13/activism-on-social-media-varies-by-race-and-ethnicity-age-political-party/ [https://perma.cc/WTM3-RTDV].

171. *See* Perrin, *supra* note 25 (noting the impact that social media has on exposing people to new ideas that in turn change their opinion on the subject); *see also* Miladi, *supra* note 27, at 36-51 (stating that the role of Twitter is integral in political participation and rallying efforts in both the Tunisian and Egyptian revolutions).

172. *See* Miladi, *supra* note 27, at 42, 47.

173. *See id.* at 49.

174. *See id.*

175. *See* Nussbaum, *supra* note 112, at 290.

The Capability Approach is both a creative and intuitive human-centered social policy planning tool. For substantive policy goals to be met, there must be positive involvement by the government. This amounts to active involvement allowing Internet access to be understood as part of the external component that governments must secure in order for individuals to be able to decide how to lead their lives.

B. Consequences of Adhering to Nussbaum's Capability Approach

If one accepts the above analysis, the implications for social policy planning are varied. This approach provides a framework for assessing policy choices and priorities, which is a useful tool for policymakers when faced with evaluating different approaches. Application of the Capability Approach serves as a useful policymaking tool whether one is sitting in federal, state, county, municipal, or tribal governments. The two specific examples discussed below are meant to illustrate a larger theme once the Capability Approach is accepted: there are creative and resourceful ways for government, at all levels, to actualize its positive duty to secure and promote reliable Internet access.

Although, as indicated in the Background section, Congress and the Biden Administration took concrete steps to further accessibility and cut down on costs of reliable Internet access in the first year of President Biden's term in office, the Capability Approach illuminates gaps and opportunities for movement and growth.[176] The approaches put forward in this section are particularly ripe for current discussion and ultimate execution—that is to say, there is meaningful space to make advancements. Varied government action can and should act to fill the space left open both by existing federal initiatives and powerful private-sector companies to ultimately increase Internet access throughout the United States. The purpose of the two examples below is to illustrate ways in which government action can be increased and the positive duty better actualized. At bottom, creativity and innovation from those in the community should influence policy decisions.

1. Municipal Broadband and Beyond

The obstacles faced by local communities in efforts to implement municipal broadband illustrate the ways that state government inhibits furthering both the accessibility and affordability of broadband. Understood through Nussbaum's Capability Approach, support for municipal broadband projects may be one way for federal, state, or municipal governments to fulfill their positive duties to promote the actualization of citizens' Central Capabilities through expansion of the background condition of Internet access. Therefore, the obstacles that currently exist should be removed. The principal way this should occur is through congressional action. Specifically,

176. Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 60102, 135 Stat. 429, 1182 (2021).

Congress should issue a plain statement to the FCC granting it the power to preempt state laws that seek to block or dampen the spread and accessibility of municipal broadband.[177]

Because the FCC currently has no plain statement authorization from Congress to preempt state municipal broadband restrictions, it remains an open question if such an authorization would withstand constitutional muster. However, there is precedent to suggest that it would.[178] Additionally, in *Nixon*, there was an indirect suggestion "that a clear statement might be sufficient to support such preemption."[179] At bottom, Congress should issue a clear statement rule to the FCC, allowing it to preempt state laws thwarting municipal broadband efforts. Any remaining constitutional concerns should be addressed once Congress issues the plain statement, but such delegation would likely withstand constitutional scrutiny.[180] Barring congressional action, states could still look to the Capability Approach as justification for removing restrictions and offering support for projects like municipal broadband.

Beyond support for municipal broadband, there are multiple other activities and programs Congress could engage in to further implement its positive duty to support affordable and available Internet access. For instance, Congress could hold hearings that seek to solicit and incorporate community and state needs into already existing federal broadband programs.[181] This could also extend to backing more programs that provide resources for questions and concerns as they relate to the use and functionality of the Internet more generally. Broadband literacy is an important element of furthering the reach of broadband.

2. Federal Asset Deployment

Another way to further actualize widespread Internet access is to expand the reach of federal infrastructure that is already in place. This should work in concert with municipal broadband initiatives.[182] In some regions of the country, municipal broadband is more desirable, whereas in other regions, Federal Asset Deployment might be possible. The federal government should expedite permitting for broadband infrastructure along highways and railways.[183] For example, the Federal Highway Administration recently published a rule that will allow broadband infrastructure to be installed at the

177. *See* Tennessee v. FCC, 832 F.3d 597, 611-12 (6th Cir. 2016).

178. *See* Lawrence Cnty. v. Lead-Deadwood Sch. Dist., 469 U.S. 256, 270 (1985).

179. *See id.*; *see also* Nixon v. Mo. Mun. League, 541 U.S. 125, 140 (2004) (noting that "preemption could operate straightforwardly to provide local choice").

180. If the central thrust of this Note is adopted, there would be an increase in government involvement in the distribution of Internet access. While it is possible that this may raise First Amendment concerns, such concerns fall outside the scope of this Note, but addressing them will be critical as government involvement in broadband access increases.

181. RACHFAL, *supra* note 34, at 13.

182. *See id.* at 7.

183. *See id.* at 8.

same time as road construction.[184] This is a helpful step because it will speed the process up and promote a policy of "dig once."[185] ISPs that traditionally struggle reaching rural communities would stand to benefit (or have less financial reasons not to deploy broadband to harder to reach communities) if the pre-existing infrastructure from other federal activities can be used.[186] The permitting process should be efficient, made possible through the relationship between the National Telecommunications and Information Administration ("NTIA") and various federal agencies.[187]

In sum, these two illustrations—municipal broadband and deployment of federal assets to enable private ISPs to broaden the reach of their broadband—are two distinct solutions to further broadband access that should become more ubiquitous around the country. When appreciated through the lens of Martha Nussbaum's Capability Approach, federal, state, and local governments, should marshal these tools to fulfil their positive duty: promote the background condition of furthering broadband access.[188]

IV. CONCLUSION

Representative John Lewis saw things, believed things, and fought for things before they even appeared on the horizon. He was no less accurate about the role that securing equitable Internet access would play in society.[189] Human-centered social policy planning is an important step to reaching digital equity. Nussbaum's theory provides needed insight into the positive role that must be placed on government to promote reliable Internet access. Adopting this framework would go a long way in preventing children from being forced into public parking lots to complete their schoolwork. While our need and reliance on Internet only increases, digital inequity still remains.

This Note has shown that Internet is a material background condition to human flourishing and, therefore, government must actively work to provide it. More should be done. Nussbaum's theoretical framework applied in a unique context illuminates the shortcomings of negative duty and highlights the importance of implementing policy initiatives that further the state's positive duty to provide background conditions that individuals need in order to decide how to lead their lives.

---

184. Broadband Infrastructure Deployment, 86 Fed. Reg. 68553 (Dec. 3, 2021) (to be codified at 23 C.F.R. pt. 645).

185. *See* 86 Fed. Reg. at 68555.

186. *See id.*

187. *See id.*; Agency Profile, Nat'l Telecomm. & Info. Admin, U.S. Dep't of Com., NTIA At-A-Glance 1, 3-4, 6 (2022), https://www.ntia.doc.gov/files/ntia/publications/ntia_at_a_glance_march_2022.pdf [https://perma.cc/YHX5-A4QC].

188. These represent just two examples. Other creative approaches that go beyond the scope of this project should also be considered.

189. *See* JONATHAN SALLET, BENTON INST. FOR BROADBAND & SOC'Y, BROADBAND FOR AMERICA NOW 8 (2020), https://www.benton.org/sites/default/files/BroadbandAmericaNow_final.pdf [https://perma.cc/SF57-CKM7].

Straight to the Source: Shielding a Journalist's Metadata with Federal Legislation

Julia Dacy*

TABLE OF CONTENTS

* J.D., May 2023, The George Washington University Law School. Editor-in-Chief, Federal Communications Law Journal, Volume 75. B.A., 2018, Strategic Communication and Socio-Legal Studies, The University of Denver. I would like to thank the Volume 75 Editorial Board for their dedication to this publication. I'd also like to thank my family for their support and for being the first to pique my interest in this area.

I. INTRODUCTION

The summer of 2020 was a busy time for journalists. A global pandemic raged.[1] Demands for racial justice and police reform following the deaths of Breonna Taylor and George Floyd sparked nationwide protests, and a contentious presidential election was underway.[2] As history unfolded and most Americans were locked down in their homes, journalists worked to bring crucial information to the electorate—often risking their own health and safety to do so.[3] While these events occurred on the world stage, a much more private storm was brewing at major news outlets—one that could undermine the free press this country relies on. On July 17, 2020, CNN's Executive Vice President and General Counsel, David Vigilante, received a secret order issued by a federal magistrate judge in the Eastern District of Virginia demanding that the network produce email headers from reporter Barbara Starr spanning a two-month period in 2017.[4] Vigilante was bound by a gag order that prevented him from publicly acknowledging the government's actions or discussing the situation with anyone besides the outside counsel retained by WarnerMedia.[5] The gag order explicitly prohibited Vigilante from informing Starr that the government was compelling the disclosure of her personal metadata.[6]

This was not an isolated incident. In the final weeks of the Trump Administration, the Department of Justice ("DOJ") engaged in a similar legal battle, this time ordering Google to hand over the personal data—including email logs—of four *New York Times* journalists who used Gmail accounts.[7] Any government collection of an individual's personal metadata without their knowledge raises serious privacy concerns. However, the implications of this practice on journalists are especially problematic because of how this data can be used in national security investigations.[8] In both of these situations, the

1. *See 2020 Events*, HISTORY (Dec. 21, 2020), https://www.history.com/topics/21st-century/2020-events [https://perma.cc/2GVJ-4AU2].

2. *See id.*

3. *See* Louis Jacobson & Samantha Putterman, *Best Practices for Journalists Covering the 2020 Election: A Report from the Poynter Institute,* POLITIFACT (Sept. 20, 2020), https://www.politifact.com/article/2020/sep/20/best-practices-journalists-covering-2020-election-/ [https://perma.cc/EL3E-MTM4].

4. *See* David Vigilante, *CNN Lawyer Describes Gag Order and Secretive Process Where Justice Department Sought Reporter's Email Records*, CNN (June 9, 2021, 2:46 PM), https://www.cnn.com/2021/06/09/politics/david-vigilante-cnn-email-secret-court-battle/index.html [https://perma.cc/DEU8-4PCD].

5. *See id*

6. *See id.*

7. *See* Charlie Savage & Katie Benner, *U.S. Waged Secret Legal Battle to Obtain Emails of 4 Times Reporters*, N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/04/us/politics/times-reporter-emails-gag-order-trump-google.html [https://perma.cc/Q3J9-96R9].

8. *See* E-mail from David McCraw, Senior Vice President & Deputy Gen. Couns., N.Y. Times, to author (Jan. 24, 2022, 10:23 PM EST) [hereinafter E-mail from David McCraw] (on file with author).

information sought by the DOJ was part of a leak investigation, and the agency was attempting to uncover the identities of confidential sources.[9]

No official privilege for journalists exists within the context of the First Amendment or any federal statute.[10] However, nearly every state has enacted some kind of journalist shield law that protects reporters from being held in contempt for refusing to disclose the identities of their sources.[11] When the government seeks traditional materials, like interview notes, the reporter is aware of the subpoena and is required to turn them over personally.[12] The availability of metadata presents new concerns because, with access to it, prosecutors can piece together the identities of sources without ever bringing a journalist before a grand jury.[13] Rather than having to go through the hassle of compelling a journalist to reveal a source, investigators can determine this information on their own.[14] Most concerning is the fact that metadata can be collected without the reporter's knowledge, leaving the journalist helpless in terms of protecting the source.[15] As evidenced by the experiences of CNN and *The New York Times*, a journalist can be completely unaware of requests for their own metadata if a gag order is put in place.[16] These orders undermine the effectiveness of state shield laws and compromise the safety of sources and the integrity of investigations.[17] Federal legislation that includes protections against the compelled disclosure of a journalist's metadata is the best approach to handling the new issues presented when government agencies seek access to this modern information.

The idea of a federal shield law dates back to the 1972 Supreme Court case *Branzburg v. Hayes*.[18] In a 5-4 decision, the justices ruled that there is not an absolute reporter's privilege implied in the First Amendment that allows a journalist to refuse to testify about criminal acts she witnessed before a grand jury.[19] Justice Powell's concurring opinion, however, left open the possibility of federal protection for journalists from compelled disclosure of

---

9. *See* Savage & Benner, *supra* note 7.

10. *See* Jonathan Peters, *Shield Laws and Journalist's Privilege: The Basics Every Journalist Should Know*, COLUM. JOURNALISM REV. (Aug. 22, 2016), https://www.cjr.org/united_states_project/journalists_privilege_shield_law_primer.php [https://perma.cc/K6XF-RRP8].

11. *See Shield Law Statute*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/privilege-sections/a-shield-law-statute/ [https://perma.cc/M65Z-58FZ] (last visited Jan. 25, 2022).

12. *See Introduction to the Reporter's Privilege Compendium*, REPS. COMM. FOR FREEDOM OF THE PRESS (Nov. 5, 2021), https://www.rcfp.org/introduction-to-the-reporters-privilege-compendium/ [https://perma.cc/J2VD-MRZZ].

13. Videoconference Interview with David McCraw, Senior Vice President & Deputy Gen. Couns., N.Y. Times (Jan. 4, 2022).

14. *Id.*

15. *See* Savage & Benner, *supra* note 7.

16. *See id.*

17. *See* JULIE POSETTI, UNESCO, PROTECTING JOURNALISM SOURCES IN THE DIGITAL AGE 8 (2017), https://unesdoc.unesco.org/ark:/48223/pf0000248054/PDF/248054eng.pdf.multi [https://perma.cc/WPK7-K7HE].

18. *See* Elizabeth Soja, *Supporting a Shield*, 31 NEWS MEDIA & L., no. 1, Winter 2007, at 7, 8.

19. *See* Branzburg v. Hayes, 408 U.S. 665, 702-04 (1972).

certain information.[20] Justice Powell explained that the need for testimony on criminal matters must be weighed against possible infringements on freedom of the press.[21] He stated, "[T]he courts will be available to newsmen under circumstances where legitimate First Amendment interests require protection."[22] In the year following the *Branzburg* decision, Congress introduced 65 bills addressing the forced disclosure of information by news media.[23] Yet, almost fifty years have passed since *Branzburg*, and the country is still without a federal statute and uniform guidance on this issue.[24] In the decades since the decision, technology has dramatically changed the way reporters do their jobs.[25] When *Washington Post* reporter Bob Woodward wished to speak with Watergate source Mark Felt—also known as Deep Throat—he moved a red flag to the balcony of his apartment.[26] The two would then meet in person at an underground parking garage.[27] While this may seem like something out of Hollywood rather than the history books, these tactics helped conceal Felt's identity for over three decades.[28] These days, journalists rely on a number of modern methods, including email and messaging apps, to communicate with sources.[29] While the Committee to Protect Journalists suggests digital best practices for source protection, such as enabling two-factor authentication for devices and using encrypted messaging applications like WhatsApp, none of these methods are as foolproof as the Watergate-era meetups.[30] Shield legislation must address both a journalist's rights when physically present in front of a grand jury and in regards to the digital fingerprints they leave behind. The recent struggles between the government and news organizations provide a renewed sense of urgency for passing this kind of legislation and making sure that it addresses our twenty-first century concerns.

The government's ability to gather a journalist's metadata from a news organization or their Internet service provider threatens the sanctity of the relationship between the media and their confidential sources because law enforcement can use this information to uncover the identity of a source with relative ease.[31] This Note compares various legal frameworks for protecting sources and argues that federal legislation is necessary because alternatives, such as relying on DOJ policy or amending state shield laws to include data

20. *See id.* at 710 (Powell, J., concurring).
21. *See id.*
22. *Id.*
23. *See* Soja, *supra* note 18, at 8.
24. *See id.* at 8-9.
25. *See* POSETTI, *supra* note 17, at 104.
26. Bob Woodward, *How Mark Felt Became 'Deep Throat'*, WASH. POST (June 20, 2005), https://www.washingtonpost.com/politics/how-mark-felt-became-deep-throat/2012/06/04/gJQAlpARIV_story.html [https://perma.cc/7RJM-Y4WT].
27. *Id.*
28. *See id.*
29. *See Digital and Physical Safety: Protecting Confidential Sources*, COMM. TO PROTECT JOURNALISTS, (Nov. 22, 2021, 10:56 AM), https://cpj.org/2021/11/digital-physical-safety-protecting-confidential-sources/ [https://perma.cc/TDW6-7TPB].
30. *See id.*
31. *See* POSETTI, *supra* note 17, at 26.

protections, would be inefficient and yield inconsistent results. The implications of this kind of data collection are even more problematic than with traditional materials because metadata is particularly useful in government investigations involving national security, which can be used as an excuse to forgo notice to the journalists involved.[32] As such, DOJ policy makes metadata relating to national security extremely vulnerable to collection without the affected reporter's knowledge.

This Note will begin by defining metadata and exploring the ways in which government agencies can access this information without a reporter's knowledge. The Background section will also provide a comparison of present and past administrative policies on the collection of such data from reporters directly and from the Internet service providers they contract with. This Note will analyze how this kind of metadata plays a role in national security investigations and why this makes it susceptible to government collection. It will also compare existing state shield laws to demonstrate the inconsistencies that exist across jurisdictions and make a case for a federal solution. Finally, this Note will outline the provisions to include in a federal shield law and how Congress can overcome the challenges that have previously prevented such legislation from being passed.

II. BACKGROUND

A. The Importance of Metadata

1. Defining Metadata

Metadata is commonly described as data concerning data because it explains and helps locate the origins of an information source.[33] The difference between content information and metadata can be difficult to discern.[34] However, making this distinction clear is vital.[35] Metadata does not describe the content of a digital communication, such as the actual text of an email correspondence.[36] Rather, it includes information about the nature of that communication, including the sender and recipient.[37] This metadata is often embedded directly in a piece of digital information, such as an HTML document or image file, so that they can be updated together over time.[38]

32. 28 C.F.R. § 50.10(a)(2) (2015).

33. *See* NAT'L INFO. STANDARDS ORG., UNDERSTANDING METADATA 1 (2004), https://web.archive.org/web/20141107022958/http://www.niso.org/publications/press/UnderstandingMetadata.pdf [https://perma.cc/F9A4-VBKK].

34. *See* Josephine Wolff, *Newly Released Documents Show How Government Inflated the Definition of Metadata*, SLATE (Nov. 20, 2013, 10:45 AM), https://slate.com/technology/2013/11/dni-patriot-act-section-215-documents-show-how-government-inflated-metadata-definition.html [https://perma.cc/V4ZU-GZ7K].

35. *See id.*

36. *See* Geneva Ramirez, Note, *What* Carpenter *Tells Us About When a Fourth Amendment Search of Metadata Begins*, 70 CASE W. RSRV. L. REV. 187, 191 (2019).

37. *See id.* at 198.

38. *See* UNDERSTANDING METADATA, *supra* note 33.

While content—like the body of an email—is clearly protected by the Fourth Amendment, many have argued that metadata is not.[39] The Electronic Communications Privacy Act of 1986 ("ECPA") granted the Director of the FBI access to "electronic communication transactional records" when needed for counterintelligence investigations.[40] The Act was passed while the Internet was still in its infancy, so it focused largely on telephone communications.[41] For instance, Chapter 206 of the Act prohibits the use of pen registers—"a device which records or decodes electronic or other impulses which identify the numbers dialed…on the telephone line"—without a court order.[42] However, those definitions were updated with the passage of the 2001 USA PATRIOT Act, which aimed to encompass new technologies and allow for the advent of technologies not yet in existence.[43] The PATRIOT Act revised the definition of pen register to include, "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[44] This essentially expanded the meaning of metadata to include anything that is not clearly content[45] and allowed government entities to authorize broad collections of metadata by the government.[46]

2. Metadata and Journalism

This non-content definition of metadata played a crucial role in the DOJ's attempt to obtain the metadata of *New York Times* reporters from Google.[47] The court order issued by the United States District Court for the District of Columbia mandated that Google disclose information about the subscribers of the accounts listed, which included names, addresses, means of payment, and the existence of geolocation records associated with the users.[48] Additionally, Google was ordered to turn over "[a]ll records and other information relating to the Account(s) (except the contents of the communications)" from the specified time period.[49] In CNN's case, a federal magistrate judge for the Eastern District of Virginia ordered the news organization to produce a reporter's email headers.[50] Email headers use

39. *See* Ramirez, *supra* note 36, at 189.
40. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2709.
41. 18 U.S.C. § 3126.
42. *Id.*
43. *See* Wolff, *supra* note 34.
44. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 290.
45. *See* Wolff, *supra* note 34.
46. *See id.*
47. *In re* Application of USA for 2703(d) Order for Six Email Accounts Serviced by Google, LLC for Investigation of Violation of 18 U.S.C. §§ 641 and 793, No. 20-sc-3361-ZMF, at 3-5 (D.D.C. Dec. 30, 2020) (order granting 2703(d) request) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).
48. *See id.* at 3-4.
49. *See id.* at 4.
50. *See* Vigilante, *supra* note 4.

metadata to provide details about the communication.[51] A full header can include the true IP address of the computer that the email was sent from, timestamps, the email addresses of senders and recipients, and even the subject lines of the message.[52]

Email metadata like this can serve many useful purposes, such as identifying the origin of a spam message.[53] However, issues arise when the government is able to access this information without a journalist's consent or knowledge. Journalism has long been regarded as the Fourth Estate, an integral democratic force working to inform the electorate and hold government officials accountable.[54] If the government—the very entity that reporters are supposed to provide a check on—can trace the course of an investigation and obtain the identity of sources, this purpose is undermined. When a reporter's ability to protect a source is compromised, the adverse effects on journalism as a whole are wide-reaching.[55] Through metadata, the subjects and targets of investigations can be revealed prior to publication, allowing for cover-ups and the destruction of vital information.[56] Additionally, potential sources are less likely to contact journalists, and journalists are less likely to engage with anonymous sources if both parties are aware that information about their communications could be seized without their knowledge.[57] This places a dangerous chilling effect on the press, which is the very result the First Amendment was designed to prevent.[58] Legislation at the state level has long recognized the value of anonymous sources and sought to safeguard them from legal repercussions and the threat of physical harm,[59] but court orders demanding metadata that can reveal their identities are loopholes to the protections shield laws provide.

3. How the Government Can Access Metadata Without a Reporter's Knowledge

To fully comprehend how government access to metadata undermines freedom of the press and puts sources at risk, one must first understand how the government can gain access to this information. The DOJ's policy regarding obtaining information from the media is outlined in Section 50.10 of the Code of Federal Regulations.[60] According to the Code, the DOJ—with the Attorney General's authorization—can access information from journalists through "subpoenas, court orders . . . and search warrants." [61]

---

51. *See Interpreting Email Headers*, UNIV. OF ROCHESTER, https://tech.rochester.edu/security/interpret-email-headers/ [https://perma.cc/83VP-RRL6].
52. *See id.*
53. *See id.*
54. *See* Mark Hampton, *The Fourth Estate Ideal in Journalism History*, *in* THE ROUTLEDGE COMPANION TO NEWS AND JOURNALISM 3, 3 (Stuart Allan ed., 2010).
55. *See* POSETTI, *supra* note 16, at 8.
56. *See id.* at 8, 37.
57. *See id.* at 8.
58. *See id.*
59. *See generally Shield Law Statute*, *supra* note 10.
60. 28 C.F.R. § 50.10 (2015).
61. *Id.*

Using these tools, law enforcement officials can obtain communications records, which are defined as "the contents of electronic communications as well as source and destination information associated with communications, such as email transaction logs and local and long distance telephone connection records, stored or transmitted by a third-party communication service provider."[62] As seen in the DOJ's efforts to access the metadata of CNN and *New York Times* reporters last year, the Department is under no legal obligation to notify the affected news media professional so long as the Attorney General determines that there are compelling reasons to withhold the notice due.[63]

The ECPA governs how agencies are able to compel information from service providers.[64] While both subpoenas and court orders are important tools for seizing electronic data, they are not equally powerful.[65] Obtaining a subpoena is the more expedient approach because investigators do not need to provide cause, and a judge does not have to sign off.[66] However, subpoenas are limited to certain types of basic subscriber data.[67] Court orders and search warrants can compel more detailed information.[68] Section 2703(d) of the ECPA requires the government to present "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[69] In the case of *The New York Times*, DOJ officials wanted access to reporters' email metadata to identify sources of leaks, so they sought the more powerful 2703(d) order from a judge, as opposed to a subpoena.[70] The court determined that the government offered "specific and articulable facts" to prove that the information sought would be "relevant and material to an ongoing criminal investigation."[71]

62. *Id.*
63. *Id.*
64. 18 U.S.C. § 2703.
65. *See* Jay Greene, *Tech Giants Have to Hand over Your Data When Federal Investigators Ask. Here's Why.*, WASH. POST (June 15, 2021, 6:00 AM), https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/ [https://perma.cc/7AHS-YQD7].
66. *See id.* (noting that a federal magistrate judge was needed to sign the order in the case of the New York Times because investigators wanted to impose a gag order).
67. 18 U.S.C. § 2703; *see also* Greene, *supra* note 65.
68. *See id*.
69. 18 U.S.C. § 2703(d).
70. *In re* Application of USA for 2703(d) Order for Six Email Accounts Serviced by Google LLC for Investigation of Violation of 18 U.S.C. §§ 641 and 793, No. 20-sc-3361-ZMF, at 1 (D.D.C. Dec. 30, 2020) (order granting 2703(d) request) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).
71. *Id.*

B. Existing Protections for Journalists' Metadata

1. Administrative Policy

In the years following the Watergate scandal, the DOJ made changes to ensure that attorneys general could act in a nonpartisan manner, free to make law enforcement decisions without political pressure imposed by the President.[72] However, this kind of separation works better in theory than in practice. Former Attorney General Griffin Bell, who served in the Carter Administration and spearheaded many of the agency reforms, explained that complete independence is not possible because the DOJ has a responsibility to the President.[73] As evidenced by both the Trump and Biden Administrations' handlings of leak investigations that led to the seizing of reporters' metadata, it is common for an administration to influence agency policy.[74] Attorneys General Jeff Sessions and William Barr zealously pursued investigations involving leaks of classified information during their tenure.[75] While investigations of this nature are commonplace, the Department took a more aggressive approach than under past administrations by subpoenaing the metadata of journalists and even sitting congressmen.[76]

This practice came to an abrupt end when, six months into the Biden administration, the existence of these investigations and gag orders came to light.[77] The White House claimed that, consistent with beliefs about the independence of the DOJ, it was not aware of the gag orders until they were made public.[78] Then on June 5, 2021—just two weeks after President Biden said he would not allow the seizure of journalists' phone and email data—the DOJ announced a significant policy change.[79] The Department's spokesman, Anthony Coley, stated, "[g]oing forward, consistent with the President's direction, this DOJ—in a change to its long-standing practice—will not seek

72. *See* Joan Biskupic, *Watergate and White House Interference at DOJ*, CNN (Oct. 28, 2017, 7:37 PM), https://www.cnn.com/2017/10/28/politics/justice-department-interference/index.html [https://perma.cc/957H-5NZQ].

73. *See id.*

74. *See generally* Katie Benner et al., *Hunting Leaks, Trump Officials Focused On Democrats in Congress*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/10/us/politics/justice-department-leaks-trump-administration.html [https://perma.cc/C9GB-SSJX]; *see also* Charlie Savage & Katie Benner, *White House Disavows Knowledge of Gag Order On Times Leaders in Leak Inquiry*, N.Y. TIMES (June 7, 2021), https://www.nytimes.com/2021/06/05/us/politics/biden-gag-order-new-york-times-leak.html [https://perma.cc/AC6A-588F].

75. *See* Benner et al., *supra* note 73.

76. *See id.*

77. *See* Savage & Benner, *supra* note 73.

78. *See id.*

79. *See* Matt Zapotosky, *Amid Controversy, Justice Dept. Says It Won't Seek to Compel Journalists to Give Up Source Information*, WASH. POST (June 5, 2021, 7:44 PM), https://www.washingtonpost.com/national-security/new-york-times-justice-department/2021/06/05/0fc66026-c61d-11eb-93f5-ee9558eecf4b_story.html [https://perma.cc/V5QR-WFDQ].

compulsory legal process in leak investigations to obtain source information from members of the news media doing their jobs."[80]

There are two key pieces of this statement to break down. The first is that the Department stated the policy change was made to be consistent with President Biden's remarks.[81] This change indicates the authority that the president still holds over an agency that is intended to have significant independence. Secondly, Coley explained that this change breaks from "long-standing" Department policy.[82] This extends back further than just the Trump Administration. For instance, in 2013, a similar controversy occurred when the DOJ under President Obama seized the phone records of reporters for the Associated Press.[83] Like with many issues dictated by agency policy, there is a frustrating lack of consistency when each new administration can change longstanding practices with ease. As it stands today, a reporter's metadata is safe from government seizure, but this does nothing to protect such information in the long run. In a positive step forward, the DOJ finally amended its regulations to reflect this policy change.[84] On October 26, 2022, Attorney General Merrick Garland announced that the Department's news media policy had formally been revised to end the practice of using compulsory legal processes to obtain information collected by newsgatherers.[85] Yet, the new regulations still provide for exceptions to this rule and make only a brief mention of protections for metadata.[86] Investigative reporting often spans many years, and safeguarding this sensitive information is too important to leave up to the whims of our constantly changing political power structure. Relying on administrative policy to determine what kinds of protections are afforded to the press is an ineffective strategy that will cause the issue to be revisited every four to eight years. Instead, we need a more permanent legislative solution.

2. Data Collection from Third Parties

While tech companies often have a reputation for failing to protect their users' data, Google proved to be an unlikely ally to *The New York Times* in its conflict with the DOJ.[87] Since a gag order prevented Google from

80. *See id.*
81. *See id.*
82. *See id.*
83. *See* Charlie Savage & Leslie Kaufman, *Phone Records of Journalists Seized by U.S.*, N.Y. TIMES (May 13, 2013), https://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html [https://perma.cc/MR26-E7NN].
84. Memorandum from Merrick Garland, Att'y Gen., U.S. Dep't of Just., to All Dep't Emps. (Oct. 26, 2022), https://www.justice.gov/ag/page/file/1547041/download [https://perma.cc/ZV4F-38M6].
85. *See id.*
86. *See* Policy Regarding Obtaining Information From or Records of Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media, 87 Fed. Reg. 66239, 66240-44 (Nov. 3, 2022) (to be codified at 28 C.F.R. pt. 50).
87. *See* Joe Toscano, *Data Privacy Issues Are the Root of Our Big Tech Monopoly Drama*, FORBES (Dec. 1, 2021, 12:19 PM),

immediately informing *The New York Times* of the order issued for its reporters' metadata, legal counsel for the newspaper was not in a position to push back.[88] Per Google's own privacy policy, the company states that it will not provide users notice of requests for information until "after a legal prohibition is lifted, such as a statutory or court-ordered gag period has expired."[89] Yet, Google's legal team fought to inform counsel for *The New York Times*, and—just three months after they were initially ordered to produce the data—prosecutors permitted Google to provide this notice to the newspaper.[90] On March 2, 2021, a second order was issued which stated that Google was permitted to disclose the existence of the January 5, 2021 Order to David McCraw, Deputy General Counsel for *The New York Times*, "but that Google, its counsel, and Mr. McCraw may not share the existence or substance of either of these Orders with any other person without further approval from this court."[91]

Considering Google's success on this issue, it could be argued that having tech companies and news organizations work together to combat orders like these is an effective strategy for protecting data. However, closer inspection of the documents involved in this lengthy legal process shows exactly why this problem cannot be solved on a case-by-case basis. Even after Google was allowed to inform counsel for *The New York Times* about the subpoenas, the gag order was not lifted.[92] Instead, just as CNN's Vigilante was prevented from notifying Ms. Starr about the investigation into her emails, the Deputy General Counsel for *The New York Times* was also now bound by the same gag order placed on Google.[93] Once informed, The New York Times' counsel argued that there was no basis for continued

---

https://www.forbes.com/sites/joetoscano1/2021/12/01/data-privacy-issues-are-the-root-of-our-big-tech-monopoly-dilemma/?sh=5785a6893cfd [https//perma.cc/Z8AH-HPRA]; *see also* Savage & Benner, *supra* note 6.

88. *In re* Application of USA for 2703(d) Order for Six Email Accounts Serviced by Google LLC for Investigation of Violation of 18 U.S.C. §§ 641 and 793, No. 20-sc-3361-ZMF, at 1 (D.D.C. Dec. 30, 2020) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).

89. *See How Google Handles Government Requests for User Information*, GOOGLE PRIV. & TERMS, https://policies.google.com/terms/information-requests [https://perma.cc/S8P2-8QMJ] (last visited Jan. 27, 2022).

90. *See* Letter from Theodore J. Boutrous, Jr. & Alexander H. Southwell, Couns. to the N.Y. Times Co., Gibson Dunn & Crutcher LLP, to Tejpal Chawla, Assistant U.S. Att'y, U.S. Atty's Off. for D.C., & Adam Small, Trial Att'y, U.S. Dep't of Just., at 10 (Mar. 26, 2021) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).

91. *In re* Application of USA for 2703(d) Order for Six Email Accounts Serviced by Google LLC for Investigation of Violation of 18 U.S.C. §§ 641 and 793, No. 20-sc-3361-ZMF, at 1 (D.D.C. Mar. 2, 2021) (order granting 2703(d) request) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).

92. *Id.* at 7.

93. *Id.* at 31-32.

nondisclosure of the January 5, 2021 order,[94] but it was still not made public until June of that year.[95] This means that for six months, four reporters were kept in the dark about the requests, rendering them incapable of protecting the identity of any sources or sensitive information that could be revealed by their email metadata.[96] This further demonstrates the need for federal legislation that restricts the government's ability to retain this information, shielded by gag orders and free from pushback by the media.

C. Past Attempts at a Federal Shield Law

1. A Summary of Historical Attempts at Passing Federal Shield Legislation

A federal shield law is not a novel idea. It has been proposed countless times in the decades since *Branzburg*.[97] Despite gaining bipartisan support and various levels of traction, each attempt at passing a federal shield law has ultimately failed.[98] A number of possible reasons for this exist, as evidenced by opposition to The Free Flow of Information Act.[99] Originally introduced in 2005 by Senator Richard Lugar (R-IN), The Free Flow of Information Act would have prohibited a federal entity from demanding information from a journalist such as an employee of a newspaper or television broadcast station.[100] During a hearing on the issue by the Senate Judiciary Committee, Senator Patrick Leahy (D-VT) questioned why confidentiality would supersede the need for testimony on criminal matters.[101] Additionally, Senator John Cornyn (R-TX) raised the common question of how the definition of a covered person would be extended to individuals like bloggers—rather than

94. *See* Letter from Theodore J. Boutrous, Jr. & Alexander H. Southwell, Couns. to the N.Y. Times Co., Gibson Dunn & Crutcher LLP, to Tejpal Chawla, Assistant U.S. Att'y, U.S. Atty's Off. for D.C., & Adam Small, Trial Att'y, U.S. Dep't of Just., at 3 (Mar. 16, 2021) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]).

95. *In re* Application of the N.Y. Times Co. for Access to Certain Sealed Ct. Recs., No. 21-91 (JEB), 2021 WL 5769444, slip op. at *2 (D.D.C. Dec. 6, 2021).

96. *See* Letter from Theodore J. Boutrous, Jr. & Alexander H. Southwell, Couns. to the N.Y. Times Co., Gibson Dunn & Crutcher LLP, to Tejpal Chawla, Assistant U.S. Att'y, U.S. Atty's Off. for D.C., & Adam Small, Trial Att'y, U.S. Dep't of Just., at 4 (Mar. 16, 2021) (available at https://int.nyt.com/data/documenttools/gag-order-nyt-emails-fight/34c4f238d4010147/full.pdf [https://perma.cc/ELP2-VZ6D]). *In re N.Y. Times Co.*, 2021 WL 5769444, at *2.

97. *See generally* Soja, *supra* note 18, at 8-9 (giving an overview of past unsuccessful attempts to draft and pass a federal shield law).

98. *See Federal Shield Law Efforts*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/federal-shield-law/ [https://perma.cc/A4YS-VDBH] (last updated Sept. 12, 2013).

99. *See "Reporter's Shield Legislation: Issues and Implications" (Hearing of the Senate Judiciary Committee)*, N.Y. TIMES (July 20, 2005) [hereinafter *Reporter's Shield Legislation Hearing*], https://www.nytimes.com/2005/07/20/politics/reporters-shield-legislation-issues-and-implications-hearing-of-the.html [https://perma.cc/PJH7-P72S].

100. Free Flow of Information Act of 2006, S. 2831, 109th Cong. (2006).

101. *See Reporter's Shield Legislation Hearing*, *supra* note 98.

established journalists—who publish information.[102] Despite the fact that the forty-nine states offering some kind of protection for reporters have managed to contend with these same concerns, Congress continues to raise these objections to a federal shield law.[103] A version of The Free Flow of Information Act was introduced in the House as recently as 2017, but once again, it failed to gain any traction.[104]

2. The PRESS ACT: A New Approach to the Federal Shield Law

Bills like The Free Flow of Information Act were designed to protect journalists in a more traditional sense from having to provide testimony or produce documents related to their journalism activities.[105] Only the Protect Reporters from Excessive State Suppression Act ("PRESS Act")—introduced in the Senate in 2021—starts to addresses the role that metadata now plays in news gathering operations.[106] Along with companion legislation introduced in the House of Representatives, the PRESS Act is the latest attempt to convince Congress of the need for a federal shield law, but this time, it specifically protects data held by third parties, like Internet companies, from being seized without a reporter's knowledge.[107] If the PRESS Act had been in effect when the DOJ sought the records of reporters at *The New York Times* and CNN, the gag orders likely could not have been imposed and the conflict would not have escalated as it did. In fact, the PRESS Act was introduced in response to the unfair targeting of journalists at these very organizations.[108] The Press Act passed the House of Representatives in September 2022, but still faces an uphill battle in the Senate.[109]

102. *See id.*
103. *See id.*
104. Free Flow of Information Act of 2017, H.R. 4382, 115th Cong. § 1 (2017).
105. *See* Free Flow of Information Act of 2017, H.R. 4382, 115th Cong. § 2(a) (2017).
106. *See* Protect Reporters from Excessive State Suppression (PRESS) Act, S. 2457, 117th Cong. (2021).
107. *Id.*
108. *See* One Pager, Ron Wyden, Senator, The Protect Reporters from Excessive State Suppression [PRESS] Act, (June 28, 2021), https://www.wyden.senate.gov/imo/media/doc/PRESS%20Act%20One%20pager.pdf [https://perma.cc/6H6X-94WP].
109. *See H.R.4330 – PRESS Act*, CONGRESS.GOV., https://www.congress.gov/bill/117th-congress/house-bill/4330 [https://perma.cc/L85L-H82T] (last visited Nov. 19, 2022).

III. ANALYSIS

A. The Pitfalls of Existing Legal Protections

1. Increased Importance of Journalists' Metadata in a Post-9/11 World

In the modern world, the value of metadata is greater than that of traditional journalist materials like interview transcripts or a reporter's research notes. The government's interest in metadata and the information it provides dramatically increased after the September 11, 2001 attacks.[110] As our country's priorities shifted to address terrorism, rapidly advancing technology presented new ways for law enforcement officials to investigate national security threats.[111] Certain types of online communications, including email, social networking, and other Internet activity—and the metadata they generate—have become reliable and necessary tools for combatting national security threats.[112] In fact, metadata played a crucial part in helping the United States find and kill Osama Bin Laden.[113] The National Security Agency ("NSA") used cell phone data to identify the exact location of Bin Laden's compound in Abbottabad, Pakistan.[114] Given the vast communication network of domestic and international confidential sources that reporters often maintain, it follows that the government has an interest in tapping into that information when it comes to investigating issues of national security. The usefulness of modern metadata in dealing with these issues, and the relative ease with which it can be used to make connections about confidential communications, is what makes the information it provides distinguishable from traditional reporters' materials. Metadata's role in national security and leak investigations also explains why reporters' data is so vulnerable in this area. The DOJ guidelines list several scenarios in which the Attorney General may refuse to provide appropriate notice to an affected journalist.[115] These include if it is determined that such notice would "risk grave harm to national security or present an imminent risk of death or serious bodily harm."[116] This exception gives the agency broad discretion to avoid notifying a journalist if national security is at all implicated.[117]

---

110. *See* POSETTI, *supra* note 16, at 12.

111. *See id.*

112. *See* Cassidy Pham, *Effectiveness of Metadata Information and Tools Applied to National Security*, LIBR. PHIL. & PRAC. (ELEC. J.), Feb. 2014, at 1, 18.

113. *See id.* at 17.

114. *See* Craig Whitlock & Barton Gellman, *To Hunt Osama bin Laden, Satellites Watched over Abbottabad, Pakistan, and Navy SEALs*, WASH. POST (Aug. 29, 2013), https://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html [https://perma.cc/R22C-DWBL].

115. 28 C.F.R. § 50.10 (2015).

116. *Id.*

117. *Id.*

After 9/11, preventing terrorist attacks and improving national security took precedence over nearly every other issue.[118] Despite the fact that there has not been another terrorist attack of that size on American soil since 2001, Americans have again and again placed preventing foreign terrorism at or near the top of the public's policy priorities.[119] In 2018, seventy-three percent of American adults said that investigating terrorism should be a top priority for the White House and Congress.[120] That list has never included protecting the freedom of the press.[121] Public perception and fear should not dictate agency policy or justify putting confidential sources at risk in the course of a national security investigation. This is why federal legislation is needed. A federal shield law can provide protections for journalists and their data while also respecting the government's national security goals. Specifically, legislation can mandate notice to journalists when their data is being collected, thus providing more consistency than agency policy and preventing an abuse of the Department's discretion.

2. Further Implications of Metadata

The DOJ is not the only administrative agency with a vested interest in accessing journalists' metadata and source communications.[122] Even with the DOJ's recent change of tune on this issue, a reporter's metadata is not necessarily safe from other agencies with enforcement powers.[123] Depending on the circumstances, it is possible that agencies like the Department of Homeland Security and the Securities and Exchange Commission ("SEC") would not be bound by the DOJ's guidelines and could seek a reporter's data directly from an Internet service provider.[124] Notably, the SEC received criticism in the past for its policy regarding subpoenas against journalists.[125] While the Securities Act gives the SEC authority to subpoena witnesses and require evidence be presented,[126] the agency's official policy is to conduct these investigations in a way that respects the freedom of the press.[127] For

118. *See* John Gramlich, *Defending Against Terrorism Has Remained a Top Policy Priority for Americans Since 9/11*, PEW RSCH. CTR. (Sept. 11, 2018), https://www.pewresearch.org/fact-tank/2018/09/11/defending-against-terrorism-has-remained-a-top-policy-priority-for-americans-since-9-11/ [https://perma.cc/KY2Z-CJPA].

119. *See id.*

120. *See id.*

121. *See id.*

122. *See* E-mail from David McCraw, *supra* note 8.

123. *See generally* OFF. OF LEGAL POL'Y, U.S. DEP'T OF JUST., REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES, PURSUANT TO P.L. 106-544, SECTION 7 (2002) [hereinafter REPORT TO CONGRESS].

124. *See* E-mail from David McCraw, *supra* note 8.

125. *SEC Subpoenas Target Whistle Blowers' Email with Reporters*, REPS. COMM. FOR FREEDOM OF THE PRESS (June 28, 2010) [hereinafter *SEC Subpoenas Target Whistle Blowers' Email*], https://www.rcfp.org/sec-subpoenas-target-whistle-blowers-e-mail-reporters/ [https://perma.cc/2WYS-TJJX].

126. *See* REPORT TO CONGRESS, *supra* note 122, at 173-75.

127. *See* Press Release, U.S. Sec. & Exch. Comm'n, Policy Statement of the Securities and Exchange Commission Concerning Subpoenas to Members of the News Media (Apr. 12, 2006), http://www.sec.gov/news/press/2006/2006-55.htm [https://perma.cc/ZDV3-8TQU].

instance, the agency is required to notify journalists of the requests for information and work alongside the media to tailor the subpoenas to include only "essential information."[128] In practice, these promises often fall flat. In 2010, just four years after writing these assurances into agency policy, the SEC attempted to find a loophole to its own guidelines.[129] The SEC wanted access to communications between two whistleblowers and *The Dow Jones* reporters with whom they had contact.[130] Rather than compel the reporters to turn over this information, the SEC subpoenaed the whistleblowers and required them to provide copies of emails sent to the journalists.[131] This demonstrates once again that agency policy cannot be relied on to protect any source communications, whether it be the content of emails or the metadata that explains them. When something is valuable to a government agency, it will find a way to obtain that information in the absence of a federal shield law that explicitly disallows such action.

B. Advantages of Federal Legislation Over State Legislation

1. Inconsistency in Existing State Shield Law Protections

In the absence of a federal shield law, states have been left to deal with the issue of protecting journalists from appearing before grand juries or from having to reveal their sources.[132] This means that there are currently forty-nine state laws addressing this issue in forty-nine different ways.[133] The most significant difference between existing state protections for journalists is that some confer an absolute privilege, while other jurisdictions acknowledge only a limited or qualified privilege.[134] The negative impact of this inconsistency is most evident in jurisdictions with incompatible state laws such as the Ninth Circuit.[135] California's protections for journalists are outlined in Section 1070 of the state's Evidence Code.[136] This shield law prevents "[a] publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service, or any person who has been so connected or employed" from being held in contempt for refusing to identify a source.[137] On its face, this law appears to provide strong protections for journalists facing compelled disclosure of information. However, in *Delaney v. The Superior Court of Los Angeles County*, the California Supreme Court

128. *See id.*
129. *See SEC Subpoenas Target Whistle Blowers' Email*, *supra* note 125.
130. *See id.*
131. *See id.*
132. *See Shield Law Statute*, *supra* note 10.
133. *See id.*
134. *See id.*
135. *See id.*
136. CAL. EVID. CODE § 1070 (West 2022).
137. *Id.*

recognized a significant limitation of this protection in criminal cases.[138] First, the court found that the California Evidence Code had not in fact created a reporter's privilege.[139] Instead, the court held that the rule created only an immunity from contempt that can be easily overcome if a defendant shows that the reporter's information could be helpful, even if it does not go to the "heart of the case."[140] So, if the court agrees with a defendant that the information sought is at all relevant, the reporter can be held in contempt if she refuses to disclose it.

While California's shield law is significantly hampered by the *Delaney* decision, other states in the Ninth Circuit have much more protective legislation.[141] For instance, Oregon's shield law protects against compelled disclosure and goes a step further by stating that a media professional's work product and work premises "shall [not] be subject to a search by a legislative, executive or judicial officer or body."[142] While California's immunity can be overcome in criminal cases by a mere showing that the information is helpful, a criminal defendant in Oregon has to show that the reporter's information is both material and favorable.[143] These crucial differences between legislation within the same circuit highlight why trying to solve a federal problem on the state level leads only to frustration and confusion, as reporters from neighboring states can face drastically different consequences for similar actions.[144]

2. Interpretations of Conflicting State Laws in Federal Court

Journalism, even at the local level, inherently involves issues of national importance that transcend state boundaries. As a result, cases in which a reporter's privilege could be invoked may end up in federal court through diversity jurisdiction or the existence of a federal question.[145] This means that each U.S. circuit is attempting to interpret and apply this legislation.[146] In non-diversity cases, federal courts are not bound by state-granted privileges[147] but can take notice of them regardless. For instance, in *Riley v. City of Chester*, the Third Circuit encountered a case addressing when

138. *See* Delaney v. Superior Ct., 789 P.2d 934 (Cal. 1990) (en banc).

139. *Id.* at 939 n.6.

140. *Id.* at 948.

141. *See Shield Law Statute*, *supra* note 10.

142. OR. REV. STAT. ANN. § 44.520 (West 2022).

143. *See* Duane A. Bosworth & Derek D. Green, *Oregon: Reporter's Privilege Compendium*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/privilege-compendium/oregon/ [https://perma.cc/A3TE-8YXX] (last visited Jan. 22, 2022); *see also* State *ex rel.* Meyers v. Howell, 740 P.2d. 792, 797 (Or. Ct. App. 1987).

144. *Compare Howell*, 740 P.2d. at 797 (holding that the state's media shield law protected a reporter from disclosing photographs because the accused failed to show how the information would be "material and favorable" to their case), *with Delaney*, 789 P.2d. at 953.

145. 28 U.S.C. §§ 1331-32.

146. *See generally Shield Law Statute*, *supra* note 10.

147. FED. R. EVID. 501 ("The common law—as interpreted by the United States courts in the light of reason and experience—governs a claim of privilege.").

a reporter can be compelled to reveal a source's identity.[148] While not bound by the existing Pennsylvania shield law, the court noted that "neither should we ignore Pennsylvania's public policy giving newspaper reporters protection from divulging their sources."[149] The court in this case chose to give credence to the state shield law in a federal case.[150] This lack of uniformity across the states and in court interpretations leads to a mess of inconsistent definitions and understandings of a reporter's privilege in federal cases.

3. Compelling Disclosure by an Out-of-State Witness

Due to the transitory nature of journalists' work, which involves traveling, communicating with sources across different states, and reporting on national issues, it is often unclear which state's protections apply in any given situation. In the 2013 case *Holmes v. Winter*, the New York Court of Appeals refused to compel reporter Jana Winter to testify in the trial of Aurora shooter James Holmes.[151] Winter lived and worked in New York City, but she was reporting on the Colorado case.[152] Since New York has an absolute privilege for reporters while Colorado offers only qualified protections against compelled disclosure of sources, this case highlights the challenges of relying on state solutions to solve interstate matters.[153]

As it stands today, existing state shield laws do not include explicit language protecting metadata.[154] Amending these laws to address data privacy concerns and to require state governments to notify journalists of demands for such information would certainly be a step in the right direction. However, even if states begin to add metadata protections to their shield laws, such a solution would really only scratch the surface of the issue. As previously discussed, metadata is particularly valuable to the government in national security investigations, which falls under the jurisdiction of the federal government rather than the states.[155] State prosecutors do not typically handle the matters in which metadata is most sought after.[156] Ultimately, the protection of journalists and their metadata is a federal problem that demands a federal solution.

148. Riley v. City of Chester, 612 F.2d. 708, 710 (3d Cir. 1979).
149. *Id.* at 715.
150. *Id.*
151. *See* Holmes v. Winter, 3 N.E.3d 694, 707 (N.Y. 2013) (holding that a journalist cannot be compelled to testify in a jurisdiction that offers less protection for reporters because it "would offend the core protection of the [New York] Shield Law, a New York public policy of the highest order").
152. *Id*. at 696.
153. *Id.*
154. *See Introduction to the Reporter's Privilege Compendium*, *supra* note 11.
155. *See* E-mail from David McCraw, *supra* note 7.
156. *See id.*

C. Feasibility of Federal Legislation

1. Challenges with Defining a Journalist

While a federal shield law provides the best protection for journalists and their data, there are a few key challenges to confront when drafting this kind of legislation. One of the most common justifications given for why Congress has yet to pass any of the proposed legislation on this issue is that defining a journalist is too difficult in today's world.[157] This is where analyzing state shield laws can be helpful. Each of the forty-nine states that has established some kind of protection for journalists has had to answer this question, and some have done so better than others.

An analysis of Hawaii's complicated history trying to provide protection for journalists demonstrates the challenges lawmakers face in drafting this kind of legislation. In 2008, the Hawaii legislature enacted a shield law that had one of the broadest definitions of a covered journalist.[158] In addition to providing protection for traditional journalists "employed by . . . any newspaper or magazine," the law also included a caveat for other individuals who "regularly and materially participated in the reporting or publishing of news or information of substantial public interest for the purpose of dissemination to the general public by means of tangible or electronic media."[159] The law stipulated that a non-traditional journalist's role must be demonstrated by clear and convincing evidence.[160] Unfortunately, the bill expired in 2011, and despite a two-year extension, it was eventually repealed, leaving the state without any shield law.[161] A permanent law was not adopted, in part, because lawmakers disagreed over extending protections to non-traditional journalists like bloggers.[162] This is the same dispute that has effectively killed each past attempt at a federal shield law. In 2013, when Congress last grappled with this issue, debate over extending protections to non-traditional journalists halted any progress on the legislation.[163]

Minnesota's shield law, the Minnesota Free Flow of Information Act, focuses more on defining the act of journalism rather than the profession of a journalist.[164] The statute explains that:

---

157. *See* Dylan Byers, *Senators Debate Definition of 'Journalist'*, POLITICO (Aug. 2, 2013, 1:34 PM), https://www.politico.com/blogs/media/2013/08/senators-debate-definition-of-journalist-169824 [https://perma.cc/4JUL-FH85].

158. *See* HAW. REV. STAT. § 621-2(b)(1) (2008) (repealed 2013).

159. *Id.*

160. § 621-2(b).

161. *See* John P. Duchemin, *Hawaii: Reporter's Privilege Compendium*, REPS. COMM. FOR FREEDOM OF THE PRESS, https://www.rcfp.org/privilege-compendium/hawaii [https://perma.cc/YV35-CLNV] (last visited Jan. 15, 2022).

162. *See Hawaii Shield Law Will Expire After Lawmakers Unable to Reconcile Competing Bills*, REPS. COMM. FOR FREEDOM OF THE PRESS (May 3, 2013), https://www.rcfp.org/hawaii-shield-law-will-expire-after-lawmakers-unable-reconcile-compe/ [https://perma.cc/928X-W7YH].

163. *See* Byers, *supra* note 157.

164. MINN. STAT. §§ 595.021-.025 (2021) (Minnesota Free Flow of Information Act).

> [N]o person who is or has been directly engaged in the gathering, procuring, compiling, editing, or publishing of information for the purpose of transmission, dissemination or publication to the public shall be required . . . to disclose in any proceeding the person or means from or through which information was obtained, or to disclose any unpublished information procured by the person in the course of work or any of the person's notes, memoranda, recording tapes, film or other reportorial data whether or not it would tend to identify the person or means through which the information was obtained.[165]

The scope of this statute unequivocally covers all traditional reporters but does not require that someone be formally employed as a journalist to receive protection. While the language in the Minnesota law is less explicit than Hawaii's original legislation, it leaves enough room for the courts to expand protection to non-traditional journalists.

Connecticut's shield law, on the other hand, defines news media narrowly as "[a]ny newspaper, magazine or other periodical, book publisher, news agency, wire service, radio or television station or network, cable or satellite or other transmission system or carrier, or channel or programming service for such station, network, system or carrier, or audio or audiovisual production company," and those employed by such companies.[166] This definition leaves the courts with less leeway to extend protection to bloggers and other non-traditional journalists. In fact, while case law has not fully addressed the scope of this definition, the Superior Court of Connecticut has stated that "the privilege is specific and limited," applying only to a "special class" of members of the news media, not including Internet blog sites.[167]

While it is true that living in a world where everyone walks around with a camera in their pocket has significantly changed the practice of journalism, technological progress is not a reason to avoid redefining the role. Instead, our evolving understanding of technology, data, and the role of the media should provide motivation for Congress to once and for all tackle these complicated issues. A federal shield law should follow the lead of states like Minnesota and include a definition of news media that is not conditioned on employment by a news organization. The PRESS Act provides a fairly comprehensive definition of a covered journalist that includes "a person who gathers, prepares, collects, photographs, records, writes, edits, reports, or publishes news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public."[168] In a final version of federal legislation, this definition could be further

165. § 595.023.

166. CONN. GEN. STAT. § 52-146t(a)(2)(A) (2013) (Connecticut Shield Law).

167. State v. Buhl, No. S20NCR10127478S, 2012 WL 4902683, at *7 n.5 (Conn. Super. Ct. Sept. 25, 2012), *aff'd in part, rev'd in part*, 100 A.3d 6 (Conn. App. Ct. 2014), *aff'd in part, rev'd in part*, 138 A.3d 868 (Conn. 2016).

168. Protect Reporters from Excessive State Suppression (PRESS) Act, S. 2457, 117th Cong. §2(1) (2021).

strengthened by adding Hawaii's "by means of tangible or electronic media" language.[169]

2. Specific Metadata Protections Needed

After defining what a covered journalist is, the most important provision in a federal shield law would establish the scope of protected information. The purpose of the PRESS Act is to protect "data held by third parties like phone and Internet companies from being secretly seized by the government."[170] Yet, the actual legislation does not specifically mention data. Instead, it refers to "any information identifying a source who provided information as part of engaging in journalism, and any records, contents of a communication, documents, or information that a covered journalist obtained or created as part of engaging in journalism."[171] It is crucial that a federal shield law make clear that this information includes both the contents of a communication and the metadata that describes it.

The PRESS Act also does not go into detail about the procedures that should be in place to assist third party service providers in processing government requests for metadata.[172] Right now, providers rely on their own internal policies for compliance with these demands.[173] In 2013, Google's Senior Vice President and Chief Legal Officer, David Drummond, outlined Google's approach to subpoenas for user data.[174] He advocated for updates to the ECPA and described the company's process of evaluating—and often rejecting—the scope of data requests.[175] Drummond explained that, "For [Google] to consider complying, it generally must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law . . . . If it's overly broad, we may refuse to provide the information or seek to narrow the request."[176] A federal shield law needs to go into explicit detail about how that scope should be defined. The PRESS Act vaguely states that compelled information should be "narrowly tailored in subject matter and period of time covered so as to avoid compelling the production of peripheral, nonessential, or speculative information."[177]

---

169. HAW. REV. STAT. § 621-2(b)(1) (2008) (repealed 2013).

170. Press Release, Ron Wyden, Senator, Wyden Releases New Bill to Protect Journalists' First Amendment Rights Against Government Surveillance (June 28, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-releases-new-bill-to-protect-journalists-first-amendment-rights-against-government-surveillance [https://perma.cc/EX7F-Z6Z6].

171. Protect Reporters from Excessive State Suppression (PRESS) Act, S. 2457, 117th Cong. §2(8) (2021).

172. *Id.*

173. *See* David Drummond, *Google's Approach to Government Requests for User Data*, THE KEYWORD BY GOOGLE (Jan. 27, 2013), https://blog.google/technology/safety-security/googles-approach-to-government-requests/ [https://perma.cc/7R87-FUSS].

174. *Id.*

175. *Id.*

176. *Id.*

177. Protect Reporters from Excessive State Suppression (PRESS) Act, S. 2457, 117th Cong. §5(2) (2021).

However, it should clearly state that third-party providers and media organizations can quickly quash an overbroad subpoena or request that it be revised to seek only that information which is deemed absolutely necessary.

While the PRESS Act focuses largely on compulsory requests for data, a federal shield law must also address when the government can ask a third-party provider like Google to voluntarily turn over a journalist's data. Currently, at Google, this can be done through emergency disclosure requests made in cases where someone is in physical danger.[178] Google's terms of service state that it will grant these requests if the company believes it can prevent such harm in cases involving bomb threats, school shootings, missing persons cases, and other dangerous situations.[179] This kind of policy gives private organizations like Google a significant amount of discretion to hand over a consumer's data. When this decision is left to individual companies, there is no uniform standard for what constitutes an emergency situation, which further highlights why federal legislation on this issue is preferable to relying on internal company policies. A federal shield law should limit the government's ability to issue an emergency disclosure request for a journalist's metadata to only situations in which an individual is in *immediate* physical danger.

To prevent the government from acting in secrecy as it did with *The New York Times* and CNN, a federal shield law must require both notice to a covered journalist and the opportunity to be heard. The PRESS Act includes both of these provisions, stating that a federal entity can only compel a service provider to turn over information about a journalist's communications once the covered journalist has been given "notice of the subpoena or other compulsory request for such testimony or document from the covered service provider not later than the time at which such subpoena or request is issued to the covered service provider."[180] The Act would also give journalists the opportunity to argue against the compulsory request before the court.[181] This is crucial because it would allow journalists to explain any potential harm that a source could suffer if their identity were uncovered.

Certain exceptions to the notice requirement above should exist when necessary to prevent significant harm. However, the government cannot be allowed to secretly seize this information under the vague guise of national security concerns. This is another reason why a federal shield law is preferable to relying on DOJ Guidelines. Under § 50.10 of the Code of Federal Regulations, the Attorney General must only have "compelling reasons" for withholding notice to "protect the integrity of the investigation."[182] Federal legislation, on the other hand, could specify an exact legal standard that law enforcement would have to meet before the notice requirement is waived. The PRESS Act, for example, would allow for a forty-five day delay of notice "if the court involved determines there is clear and convincing evidence that such

178. *See How Google Handles Government Requests for User Information*, *supra* note 88.
179. *Id.*
180. S. 2457, § 4(c)(1)(A).
181. S. 2457, § 4(c)(1)(B).
182. 28 C.F.R. § 50.10 (2015).

notice would pose a clear and substantial threat to the integrity of a criminal investigation, or would present an imminent risk of death or serious bodily harm."[183] Notice could only be delayed further, and not by more than forty-five days at a time, by the presentation of new clear and convincing evidence.[184] Including this clear and convincing standard in a federal shield law would prevent abuses of discretion by the Attorney General while still recognizing the delicate national security concerns that need to be considered.

3. Overcoming Political Hurdles to Passing a Federal Shield Law

The increasing importance of metadata will continue to lead to battles between the government and news organizations if Congress declines to address these issues head on. A federal shield law protecting journalists is hardly a radical proposal. Moreover, expanding on previously proposed shield laws in order to address data privacy concerns is simply a way of bringing these past attempts into the twenty-first century. This is a largely bipartisan issue that has garnered support from notable politicians on both sides of the aisle, from Jamie Raskin (D-MD-08) to Jim Jordan (R-OH-04) and former Republican Vice President Mike Pence.[185] As such, there is no reason why legislation of this kind should continue to fail. Just as the Watergate scandal sparked significant DOJ reform, the recent fight over access to reporters' data should provide the impetus needed to finally pass a federal shield law.

IV. CONCLUSION

When debates surrounding shield laws first began after *Branzburg v. Hayes*, legislators could not contemplate the role that data would eventually play in our lives. Metadata, in many ways, reveals more information about a journalist's work than their traditional notes and other investigative materials ever could. As such, it should be afforded certain protections from government seizure. The best option for doing this is to finally pass a federal shield law, similar to the now-stalled PRESS Act, but with more explicit provisions requiring law enforcement to provide notice to journalists when this metadata is sought for an investigation. The cloak of secrecy allowed by gag orders, like the ones placed on Google and major media organizations last year, prevents journalists from being able to protect the identity of their sources and keep them out of harm's way. Preserving the sacred relationship between reporters and confidential sources is vital to a healthy democracy and a free press. Thus, we cannot rely on inconsistent DOJ policy or a state-by-state framework to take on this challenge. Finally passing a comprehensive

183. S. 2457, § 4(c)(2)(A).
184. S. 2457, § 4(c)(2)(B).
185. Press Release, Jamie Raskin, Representative, Reps. Raskin & Jordan Introduce Bipartisan Federal Press Shield Law (Nov. 14, 2017), https://raskin.house.gov/2017/11/reps-raskin-jordan-introduce-bipartisan-federal-press-shield-law [https://perma.cc/FQ6U-MW98].

federal shield law that encompasses data protection is the most effective way to ensure a journalist's confidential sources are protected.

Communications Law: Annual Review

Staff of the Federal Communications Law Journal

TABLE OF CONTENTS

City of Austin, Texas v. Reagan National Advertising of Austin, LLC, et al.

Alexander Goodrich

142 S. CT. 1464 (2022)

In *City of Austin, Texas v. Reagan National Advertising of Austin, LLC., et al.,* the Supreme Court affirmed the power of local municipalities to regulate highway billboards.[1] The decision also provided an illustration of the First Amendment distinction between content-neutral and content-based regulations articulated in *Reed v. Town of Gilbert*.[2]

I. BACKGROUND

Reagan National Advertising of Austin ("Reagan") and Lamar Advantage Outdoor Company ("Lamar") owned and operated multiple billboards that displayed various commercial advertisements and non-commercial messages around the city of Austin, Texas.[3] Like many other municipalities around the country, the City of Austin ("City") regulates the placement and display of billboards and signs.[4] To regulate safety and local aesthetics, the City drew a distinction between off-premises signs, or signs that direct the reader to a separate location than that of the sign (such as a roadside billboard advertising a local restaurant) and on-premises signs, or

1. City of Austin v. Reagan Nat'l Advert. of Austin, LLC, 142 S. Ct. 1464, 1472 (2022).
2. Reed v. Town of Gilbert, 576 U.S. 155, 172 (2015).
3. *See City of Austin*, 142 S. Ct. at 1468-69.
4. *See id.* at 1469-70. In the Highway Beautification Act of 1965, Congress delegated to the States the power to regulate off-premises signs, such as billboards that promote ideas, products, or services located elsewhere than the location of the sign. *See* 23 U.S.C. § 131(a)-(f).

signs that direct the reader to the same location (such as a sign on the face of a restaurant that advertises that same restaurant).[5]

In 2017, the City of Austin passed a law that "prohibited the construction of any new off-premises signs" but grandfathered in those off-premises signs that existed at the time so long as the off-premises signs were not altered in a way to increase their conspicuity, such as by digitization.[6] This case was initiated when the City of Austin denied Reagan's permit application to digitize its off-premises signs.[7]

Reagan sued the City in state court for violating his First Amendment right to free speech, and Lamar intervened, both seeking declaratory judgements finding the off-premises versus on-premises distinction unconstitutional.[8] The trial court summarily dismissed Lamar and Reagans' request, but the Fifth Circuit reversed the lower court's decision, reasoning that the off/on-premises distinction required a state agent to inquire as to "who is the speaker and what is the speaker saying."[9] Therefore, the court reasoned, the content-based regulation should be invalidated because it could not survive strict scrutiny.[10] The City of Austin petitioned for certiorari, which the Supreme Court granted.[11]

II. ANALYSIS

This case turned on determining the level of scrutiny to apply in analyzing the City's distinction between off-premises and on-premises signs.[12] In doing so, the Supreme Court was required to determine whether the regulation prohibiting the digitization of off-premises signs was content-neutral, requiring intermediate scrutiny, or content-based, which would require strict scrutiny.[13]

---

5. *See City of Austin*, 142 S. Ct. at 1468-69. While not directly at issue for respondents, there was a third type of sign implicated by this law: a subset of signs displayed on commercial premises that direct the reader to another separate premises. *See id.* at 1480-81 (Alito, J., dissenting in part and concurring in part). For example, the off-premises distinction might apply to a small sign in a coffee shop window that directs customers to "Visit the local park for free ice-cream." *See id*. Justice Thomas, joined by Justices Gorsuch and Barrett in his dissenting opinion, opined on the notion that the regulation would reach signs whose location information is also protected speech, such as a sign on a coffee shop that reads "Come to City Hall to Vote No on Prop. X." *See id.* at 1484 (Thomas, J., dissenting) ("[S]uppose the sign says, 'Go to Confession.' After examining the sign's message, an official would need to inquire whether a priest ever hears confessions at that location. If one does, the sign could convey a permissible 'on-premises' message. If not, the sign conveys an impermissible off-premises message.").

6. *See id.* at 1469-70 (majority opinion).

7. *See id.* at 1470.

8. *City of Austin*, 142 S. Ct. at 1470.

9. *Id.* (quoting Reagan Nat'l Advert. of Austin, Inc. v. City of Austin, 972 F.3d 696, 705 (5th Cir. 2020)).

10. *See id*. at 1471.

11. *See id.* at 1471.

12. *See id.* ("[A]bsent a content-based purpose or justification, the City's distinction is content-neutral and does not warrant the application of strict scrutiny.").

13. *See id.* at 1470-72.

Respondents' main substantive arguments were focused on the Court's 2015 decision in *Reed v. Town of Gilbert*.[14] Reagan argued that *Reed* stood for the proposition that regulations focused on the "function or purpose"[15] of a sign were content-based regulations and presumptively invalid.[16] Thus, they argued, regulations based on the purpose of a sign (here, whether the sign's purpose is to direct the reader to a local, or satellite, location) contravene the First Amendment's Free Speech Clause.[17]

The Majority disagreed, holding that the sign code regulation was content-neutral and would receive intermediate scrutiny.[18] The Court reasoned that, unlike the sign code provision at issue in *Reed*, the City of Austin's regulation did not single out any topic or subject matter for differential treatment.[19] Rather, the location-based distinction was more similar to a permissible time-place-manner restriction than an impermissible subject-matter restriction such as the one in *Reed*.[20] In addition, the Court noted that the vast majority of the signs in this case were commercial solicitations that have been consistently and successfully regulated more stringently than other, more protected forms of speech.[21]

In doing so, the Court abrogated the Fifth Circuit's purported rule, that a regulation is content-based if it requires the reader to evaluate the content of the message,[22] as overbroad.[23] Instead, the Court reasoned, not every regulation that hinges on the content of the speech is presumptively content-based: "[T]he City's off-premises distinction requires an examination of speech only in service of drawing neutral, location-based lines. It is agnostic as to content."[24]

---

14. *See City of Austin*, 142 S. Ct. at 1470-72; Reed v. Town of Gilbert, 576 U.S. 155 (2015) (holding that an ordinance restricting the size, number, duration, and location of temporary directional signs violated the Free Speech Clause of the First Amendment because the facially content-based regulation awarded improper selective status to certain content, earning strict scrutiny and holding that a facially content-based regulation cannot be saved by a neutral justification).

15. *City of Austin*, 142 S. Ct. at 1474 (quoting *Reed*, 576 U.S. at 163 ("[S]ome facial distinctions based on a message are obvious, defining regulated speech by particular subject matter, and others are more subtle, defining regulated speech by its *function or purpose*.") (emphasis added)).

16. *See id.* at 1475.

17. *See id.* at 1474.

18. *See id.* at 1475-76.

19. *See id.* at 1473.

20. *See id.* ("The on-/off-premises distinction is therefore similar to ordinary time, place, or manner restrictions. *Reed* does not require the application of strict scrutiny to this kind of location-based regulation.").

21. *City of Austin*, 142 S. Ct. at 1474-75 ("Most relevant here, the First Amendment allows for regulations of solicitation . . . to identify whether speech entails solicitation, one must read or hear it first.").

22. *See* Reagan Nat'l Advert. of Austin, Inc. v. City of Austin, 972 F.3d 696, 706 (5th Cir. 2020), *rev'd*, 142 S. Ct. 1464 (2022).

23. *See City of Austin*, 142 S. Ct. at 1471 ("[The Court of Appeals'] rule, which holds that a regulation cannot be content-neutral if it requires reading the sign at issue, is too extreme an interpretation of this Court's precedent.").

24. *Id.*

In a dissenting opinion penned by Justice Thomas joined by Justices Gorsuch and Barrett, Thomas focused primarily on a secondary genus of sign affected by the regulation: those located not on vacant roadsides, but those located on residential or business premises that direct customers to a different location.[25] Justice Thomas argued that the Majority created a new, unwieldy rule that misinterpreted the *Reed* holding and invented a distinction between 'subject matter' content (protected) and 'location-based' (unprotected) content.[26] Like in *Hill v. Colorado*,[27] Thomas argued, the Majority ignored the true, pointed, and "undeniably content-based"[28] effect of the regulation.[29]

Justice Alito concurred in part and dissented in part, writing that the *Reed* precedent required his concurrence because "[t]he distinction between a digitized and non-digitized sign is not based on content, topic, or subject-matter."[30] Justice Alito dissented to argue that the Majority's rule was too broad in that it left open the door for facially content-neutral laws that have unequal effects, using an example of two signs in a coffee shop window.[31] One sign that advertises a new coffee drink would be permissible, while another that reads "Attend City Council meeting to speak up about Z" would be impermissible—this clearly content-based distinction would be lawful under the Majority's interpretation.[32]

Justice Breyer wrote a concurring opinion in which he agreed with the Majority that the City's sign code provision was a content-neutral regulation under the *Reed* precedent but opined that *Reed* too strictly tied facially content-based regulations with strict scrutiny, when in reality many laws turn necessarily on the content of speech.[33] Instead, he argued, the First Amendment was written to protect the marketplace of ideas—when there is no "idea" at issue, there should be no presumption of unconstitutionality.[34]

III. CONCLUSION

The Supreme Court once again wrestled with the notion of content-based regulations in the shadow of the Free Speech Clause of the First Amendment. While the Majority relied on Reed to justify its application of intermediate scrutiny to uphold the City's location-based regulation, multiple dissenting and concurring Justices questioned the applicability of Reed's

25. *See id.* at 1483 (Thomas, J., dissenting) (stating that defining off-premises signs as signs "'advertising' . . . or . . . 'direct[ing] persons to any location not on that site' . . . sweeps in a large swath of signs, from 14- by 48-foot billboards to 24- by 18-inch yard signs." (quoting AUSTIN, TEX., CITY CODE § 25-10-3(11) (2016)).

26. *See id.* at 1485-86.

27. Hill v. Colorado, 530 U.S. 703 (2000).

28. *City of Austin*, 142 S. Ct. at 1491 (Thomas, J., dissenting) (quoting *Hill*, 530 U.S. at 742-43 (Scalia, J., dissenting)).

29. *See id.* at 1484-92.

30. *Id.* at 1480 (Alito, J., concurring in part and dissenting in part).

31. *See id*. at 1480-81 (Alito, J., concurring in part and dissenting in part).

32. *See id.* at 1480-81.

33. *See id.* at 1477-78 (Breyer, J., concurring).

34. *See City of Austin*, 142 S. Ct. at 1479.

content-based versus content-neutral distinction as applied to circumstances where the effect of the regulation is felt unequally.

Gonzalez v. Google, LLC

Catherine Ryan

2 F.4TH 871 (9TH CIR. 2021)

In *Gonzalez v. Google*, the Ninth Circuit addressed two major claims asserted against Google for the alleged role of its subsidiary, YouTube, in facilitating an ISIS terrorist attack on November 13, 2015 in Paris, France.[1] The court ultimately affirmed the district court's granting of Google's motion to dismiss, holding that 47 U.S.C. § 230 of the Communications Decency Act ("CDA") effectively immunized Google from the majority of the Plaintiffs' (collectively, Gonzalez) claims.[2] For the remaining claims, Gonzalez had failed to state a right of action under the Anti-Terrorism Act ("ATA"), 18 U.S.C. § 2333.[3] This case was argued before the United States Supreme Court on February 21, 2023 and is awaiting final disposition.[4]

I. BACKGROUND

The decedent, Nohemi Gonzalez, was a United States citizen studying in Paris, France in the fall of 2015.[5] On the evening of November 13, 2015, she was killed in a shooting at a local café by ISIS terrorists as part of a series of attacks that occurred in the city.[6] The following day, ISIS claimed responsibility for the attacks by issuing a written statement and posting a video on YouTube.[7]

The case was brought primarily by Reynaldo Gonzalez, Nohemi's father, although other family members were added as plaintiffs in the Second Amended Complaint ("SAC").[8] In the SAC, Reynaldo and family claimed that Google violated the ATA by aiding and abetting "international terrorism and provid[ing] material support to international terrorism by allowing ISIS to use YouTube."[9] Two of these claims were based on a revenue-sharing theory, whereby ISIS received payment from Google for its monetized videos.[10] Certain other claims were predicated on the broadened scope of the ATA in 2016 through the Justice Against Sponsors of Terrorism Act

1. Gonzalez v. Google LLC, 2 F.4th 871, 880-81 (9th Cir. 2021), *cert. granted*, 143 S. Ct. 80 (Oct. 3, 2022) (No. 21-1333).
2. *Id.* at 880.
3. *Id.*
4. Gonzalez v. Google LLC, No. 21-1333 (U.S. argued Feb. 21, 2023).
5. *Gonzalez*, 2 F.4th at 880.
6. *Id.* at 880-81.
7. *Id.* at 881.
8. *Id.* at 882.
9. *Id.*; 18 U.S.C. § 2333(a), (d).
10. *See Gonzalez*, 2 F.4th at 882.

("JASTA").[11] Google filed a motion to dismiss all claims for direct and secondary liability, arguing that Section 230 of the CDA bars such claims.[12] The district court agreed but granted Gonzalez leave to amend the complaint.[13]

Gonzalez then filed the Third Amended Complaint ("TAC"), which is at issue in this case.[14] In addition to the previous claims, Gonzalez alleged that Google has direct liability under Section 2333(a) of the ATA for "providing material support and resources to ISIS."[15] Google submitted a motion to dismiss the entire TAC, claiming immunity under Section 230 of the CDA, and argued in the alternative for dismissal of the Section 2333(a) direct liability claims because Gonzalez had failed to state a claim that Google had proximately caused the decedent's injuries.[16]

The district court granted the motion to dismiss on the grounds of Google's Section 230 immunity and Gonzalez's failure to plausibly allege proximate cause.[17] Gonzalez appealed.[18]

II. ANALYSIS

On appeal, the court affirmed the district court's dismissal, rejecting Gonzalez's arguments that Google does not enjoy Section 230 immunity and that Google bears direct liability under the ATA due to its revenue-sharing with ISIS.[19] The court began by framing the history and purpose of the CDA as creating immunity for "providers of interactive computer services against liability arising from content created by third parties."[20] The congressional intent at the time of the Act's passage in 1996 was to promote the free exchange of ideas in the new age of the Internet.[21] The operative provision, Section 230(c)(1), immunizes providers like Google from liability for content posted by third parties.[22]

With this framing, the court turned to Gonzalez's three arguments regarding why Google should not be given Section 230 immunity for the non-revenue-sharing claims.[23]

11. *See id.* at 889.
12. *Id.* at 882.
13. *Id.*
14. *Id.*
15. *Id.* (discussing 18 U.S.C. § 2333(a)).
16. *Gonzalez*, 2 F.4th at 882.
17. *Id.*
18. *Id.* at 883.
19. *Id.* at 880.
20. *Id.* at 886.
21. *Id.*
22. *Gonzalez*, 2 F.4th at 886.
23. *See id.*

A. Google's Immunity Under Section 230 of the CDA

1. Presumption Against Extraterritoriality

The first claim Gonzalez asserted on appeal was that the presumption against extraterritorial application precluded Section 230 from applying to their claims, as the killing of the decedent took place in France.[24] The court analyzed this claim in accordance with the Supreme Court's two-part test in *RJR Nabisco, Inc. v. European Community*.[25] The first step, "whether the presumption against extraterritoriality has been rebutted," was not at issue.[26] The court then moved to the second step: identifying the statute's focus and "whether the conduct relevant to that focus occurred in United States territory."[27] The court concluded the purpose of Section 230(c)(1) is to limit liability of interactive computer services providers (such as Google) in order to encourage them to monitor their respective websites.[28] Section 230 does this through immunizing the providers against liability for content created by third parties.[29] Given Section 230's focus on limiting liability, the relevant conduct for the extraterritorial analysis is that which incurs immunity, which in this case took place in the United States.[30] The court sided with Google, concluding that the claim involved a domestic application of Section 230 and raised no issue of extraterritorial application.[31]

2. 2016 Amending of the ATA

The second claim Gonzalez made on appeal was that when Congress amended the ATA in 2016 by enacting JASTA, it implicitly repealed Section 230.[32] The court was not so persuaded.[33] The Supreme Court held in *Branch v. Smith* that, "absent a clearly expressed congressional intention, repeals by implication are not favored."[34] Such an implied repeal as argued by Gonzalez will only be found "where provisions in two statutes are in 'irreconcilable conflict.'"[35] In considering the statutory language of JASTA, the court found no substantive provision that conflicts with Section 230.[36] Section 230 protects a narrow class of defendants from liability, protecting interactive computer services from being treated as publishers or speakers of the content

24. *See id.* at 887.
25. *See id.* (citing RJR Nabisco, Inc. v. Eur. Cmty., 579 U.S. 325, 337 (2016)).
26. *RJR Nabisco*, 579 U.S. at 337.
27. *Gonzalez*, 2 F.4th at 887 (quoting *RJR Nabisco*, 579 U.S. at 337).
28. *Id.* at 888.
29. *Id.*
30. *See id.*
31. *Id.*
32. *Id.* at 888-89.
33. *Gonzalez*, 2 F.4th at 889.
34. *Id.* (quoting Branch v. Smith, 538 U.S. 254, 273 (2003)).
35. *Id.* (quoting *Branch*, 538 U.S. at 273).
36. *Id.*

at issue.[37] JASTA included no provision to the contrary, merely expanding the scope of liability under the ATA for acts of international terrorism.[38] Therefore, the court rejected Gonzalez's claims that JASTA repealed Section 230.[39]

3. Application to ATA Claims

Gonzalez's third claim was that the ATA's right of private civil enforcement that otherwise gives rise to criminal liability cannot be immunized by Section 230.[40] Gonzalez supported this claim with the text of Section 230(e)(1), which states, "[n]othing in this section shall be construed to impair the enforcement of . . . any . . . [f]ederal criminal statute."[41] The court rejected this claim and sided with Google, concluding that Section 230(e)(1) applies only to criminal prosecution, not cases like this which are only for civil damages.[42] The court found support for this conclusion in First and Second Circuit rulings, which similarly found that Section 230(e)(1) is limited only to criminal prosecutions and, therefore, would not preclude Section 230 immunity for Google in this case.[43]

4. Application to the TAC

Concluding that Gonzalez's claims were not categorically excluded from Section 230 immunity, the court then addressed whether Google, rather than a third party, created the content addressed in the TAC and, therefore, is not afforded Section 230 immunity.[44] The court found that Google did not create or develop the ISIS content posted to YouTube, but instead merely republished it.[45] The court concluded that Google was not acting as an information content provider and was, therefore, eligible for Section 230 immunity.[46]

5. Application to the Revenue-Sharing Theory

Gonzalez's final claim regarding Section 230 immunity arose under the revenue-sharing theory: because Google shared advertising revenue with ISIS, it "should be held directly liable for providing material support to ISIS pursuant to Section 2333(a) and secondarily liable for providing substantial

37. *Id.* at 889; 47 U.S.C. § 230(c)(1).
38. *See Gonzalez*, 2 F.4th at 889.
39. *Id.* at 890.
40. *Id.*
41. *Id.*; 47 U.S.C. § 230(e)(1).
42. *Gonzalez*, 2 F.4th at 890.
43. *Id.*
44. *Id.*
45. *Id.* at 892.
46. *Id.*

assistance to ISIS pursuant to Section 2333(d)."[47] The court distinguished this claim because here, Google would be providing ISIS with material support through monetary payments, rather than simply publishing ISIS's content.[48] The court concluded that Section 230 does not necessarily preclude Gonzalez's claim based on a theory of revenue-sharing with ISIS.[49]

B. Direct and Secondary Liability Under the ATA

Given the court's finding that Section 230 does not immunize Google from liability under the theory of revenue-sharing, the court then considered whether Gonzalez sufficiently alleged claims for direct and secondary liability under the ATA.[50] The court rejected Gonzalez's theory of direct liability under Section 2333(a), concluding that the TAC offered no evidence that "Google's provision of material support appeared to be intended to intimidate or coerce a civilian population, or to influence or affect a government as required by the ATA."[51]

The court also rejected Gonzalez's theory of secondary liability, agreeing with Google that Gonzalez failed to state a claim for such a finding.[52] The operative required showing for secondary liability for aiding and abetting acts of terrorism under Section 2333(d) is that Google knowingly and substantially assisted the act of terrorism that injured the decedent.[53] While the court concluded that Gonzalez sufficiently alleged Google's "knowing" assistance through revenue-sharing, it ultimately concluded Gonzalez did not sufficiently allege Google's "substantial" assistance.[54]

III. CONCLUSION

For the foregoing reasons, the Ninth Circuit affirmed the district court's dismissal of the case, holding that for the non-revenue-sharing claims Google is eligible for Section 230 immunity and that while Google is not eligible for Section 230 immunity for the revenue-sharing claim, Gonzalez did not sufficiently allege Google's direct nor secondary liability under the ATA.[55] Gonzalez petitioned the Supreme Court of the United States for a writ of certiorari, which was granted in October 2022.[56] The Supreme Court heard the case on February 21, 2023.[57]

---

47. *Id.* at 897-98.
48. *Gonzalez*, 2 F.4th at 897-98.
49. *Id.* at 899.
50. *Id.*
51. *Id.* at 901.
52. *Id.*
53. *Id.* at 905.
54. *Gonzalez*, 2 F.4th at 907.
55. *Id.*
56. Gonzalez v. Google LLC, 143 S. Ct. 80 (Oct. 3, 2022) (No. 21-1333) (granting cert.).
57. Gonzalez v. Google LLC, No. 21-1333 (U.S. argued Feb. 21, 2023).

Content Moderation Circuit Split: NetChoice v. Attorney General, State of Florida and NetChoice v. Paxton

Emily Bernhard

34 F.4TH 1196 (11TH CIR. 2022)
49 F.4TH 439 (5TH CIR. 2022)

In 2021, both Florida and Texas enacted statutes to curtail social media platforms' ability to moderate content on their sites.[1] These statutes were intended to mitigate anti-conservative bias on social media platforms and restrict their ability to deplatform or deprioritize conservative content.[2] Plaintiffs NetChoice and Computer & Communications Industry Association (referred to collectively as "NetChoice") are trade associations that represent social media companies such as Facebook, Twitter, and Google.[3] NetChoice challenged these laws, arguing that restricting social media platforms' ability to moderate content unconstitutionally infringes on the platforms' First Amendment free speech rights.[4] The district courts in both cases granted plaintiffs' motions for preliminary injunctions and both Florida and Texas appealed these rulings.[5] The Eleventh Circuit reviewed the constitutionality of the Florida statute and affirmed the district court's decision, holding that social media platforms are private actors with constitutionally protected free speech rights, and they are acting within these rights when they make editorial judgements about the content they allow on their sites.[6] The Fifth Circuit reviewed the Texas statute and came to the opposite conclusion, holding that because these companies have such dominant market share and the vast

1. *See* S.B. 7072, 2021 Leg., Reg. Sess. (Fla. 2021) (enacted); H.B. 20, 87th Leg., 2d Spec. Sess. (Tex. 2021) (enacted).
2. NetChoice, LLC v. Att'y Gen., 34 F.4th 1196, 1208 (11th Cir. 2022) (holding that social media companies are private actors with First Amendment free speech rights and content moderation is a constitutionally protected exercise of these rights); NetChoice, LLC v. Paxton, 49 F.4th 439, 439 (5th Cir. 2022) (holding that content moderation by social media companies does not fall under the definition of speech protected by the First Amendment), *petition for cert. docketed*, No. 22-555 (U.S. Dec. 19, 2022).
3. *NetChoice*, 34 F.4th at 1207.
4. *Id.* at 1207; *Paxton*, 49 F.4th at 463.
5. *NetChoice*, 34 F.4th at 1196; *Paxton*, 49 F.4th at 439.
6. *NetChoice*, 34 F.4th at 1204.

majority of posts go unreviewed, they should be treated as common carriers that are subject to nondiscrimination requirements.[7]

I. ELEVENTH CIRCUIT

A. Background

On May 24, 2021, the State of Florida enacted S.B. 7072, which aimed to limit social media platforms' ability to moderate content on their sites.[8] S.B. 7072 was signed by Governor DeSantis in his purported effort to "fight [ ] against big tech oligarchs that contrive, manipulate, and censor if you voice views that run contrary to their radical leftist narrative."[9] NetChoice sought to enjoin enforcement of §§ 106.072 and 501.2041 of the law, which imposed liability on social media platforms for their decisions to remove content or users from their sites.[10] NetChoice argued that these provisions: (i) violate their First Amendment free speech rights, and (ii) are preempted by federal law.[11] The district court granted plaintiffs' motion to enjoin §§ 106.072 and 501.2041, which Florida appealed.[12]

B. Analysis

In its appeal, the State argued that the Florida law was not preempted by federal law and that plaintiffs' First Amendment rights were not violated because the conduct at issue does not constitute protected speech under the First Amendment.[13] NetChoice argued that by restricting social media platforms' ability to remove content from their sites, the State is both preventing the platforms from exercising editorial discretion and forcing the platforms to publish certain speech.[14] The Eleventh Circuit concluded that §§ 106.072 and 501.2041 were substantially likely to violate plaintiffs' First Amendment rights and that there was no need to consider the preemption challenge.[15]

The State argued that because these social media platforms have such significant market power and public importance, they should be treated as common carriers that have diminished First Amendment rights and must adhere to nondiscrimination requirements.[16] The Eleventh Circuit rejected the State's common carrier argument, citing § 230(c)(2)(A) of the Telecommunications Decency Act of 1996, which recognizes social media

7. *Paxton*, 49 F.4th at 459.
8. S.B. 7072, 2021 Leg., Reg. Sess. (Fla. 2021) (enacted).
9. NetChoice, LLC vs. Att'y Gen., 34 F.4th 1196, 1205 (11th Cir. 2022).
10. *Id.* at 1207.
11. *Id.*
12. *Id.* at 1208.
13. *Id.*
14. *Id.* at 1215.
15. *NetChoice*, 34 F.4th at 1209.
16. *Id.* at 1221-22.

platforms' ability to discriminate among the type of messages allowed on their platforms.[17]

Before considering whether the content-moderation restrictions violated plaintiffs' First Amendment rights, the Eleventh Circuit considered whether the law triggered the First Amendment at all.[18] The State argued that platforms are not engaging in speech that is worthy of First Amendment protection because the vast majority of content that is posted is never reviewed.[19] The Eleventh Circuit rejected this argument because the conduct at issue here deals precisely with the content that *is* reviewed by the platforms.[20]

The Eleventh Circuit compared the platforms' decisions about what content to remove or deprioritize to the kind of editorial judgment that is exercised by newspapers.[21] The platforms' unwillingness to publish certain types of content reflects their views on what is appropriate and worth disseminating to their users.[22] The Eleventh Circuit stated that the appropriate inquiry is whether a reasonable person would interpret a platform's content moderation decisions as communicating "some sort of message."[23] The Eleventh Circuit held that by exercising judgment about what messages they are willing to convey, platforms signal to users the type of online community they want to create.[24]

C. Holding

The Eleventh Circuit concluded that because social media platforms are exercising editorial judgment by making content moderation decisions, and because a reasonable person would interpret this as communicating "some sort of message," this behavior is constitutionally protected under the First Amendment.[25] Therefore, the Florida law's provisions that limit social media platforms' ability to moderate content are most likely unconstitutional.[26]

II. FIFTH CIRCUIT

A. Background

On September 9, 2021, Texas enacted HB 20, which, like the Florida law, tried to restrict social media companies' ability to regulate content on

17. *Id.* at 1221 ("Federal law's recognition and protection of social-media platforms' ability to discriminate among messages—disseminating some but not others—is strong evidence that they are not common carriers with diminished First Amendment rights.").
18. *Id.* at 1209.
19. *Id.* at 1214.
20. *Id.*
21. *NetChoice*, 34 F.4th at 1210-11.
22. *Id.* at 1210.
23. *Id.* at 1212 (quoting Coral Ridge Ministries Media, Inc. v. Amazon.com, Inc., 6 F.4th 1247, 1254 (11th Cir. 2021)).
24. *Id.* at 1213.
25. *Id.* at 1212 (quoting *Coral Ridge*, 6 F.4th at 1254).
26. *Id.* at 1214.

their platforms.[27] The law, which applies to social media companies that have over 50 million monthly active users, was largely anchored in the argument that these companies essentially function as common carriers and public forums, and thus, should not be able to censor speech on their platforms.[28] NetChoice challenged the law and sought a preliminary injunction, arguing that it substantially and unconstitutionally burdened their free speech rights.[29] The district court granted plaintiffs' motion for a preliminary injunction, and Texas appealed.[30]

B. Analysis

The Fifth Circuit rejected NetChoice's arguments that the Texas law chilled their free speech rights, finding that the statute "does not regulate the Platforms' speech at all; it protects *other people's* speech and regulates the Platforms' *conduct*."[31] The Fifth Circuit rejected plaintiffs' argument that the platforms are exercising free speech rights by moderating content on their sites and contrasted these passive decisions with the types of affirmative editorial judgments that are exercised by newspapers when they select content to publish.[32] The Fifth Circuit cited the terms of service from both Twitter and Facebook in which they tell users that they are not responsible for any content nor should the publication of content on their platform be interpreted as an endorsement.[33] The Fifth Circuit held that these companies are still empowered to speak in whatever way they want, and HB 20 only serves to prevent them from censoring others' ability to do the same.[34]

The opinion likened the platforms to "common carriers" because, rather than exercising independent editorial judgment, they serve as a conduit for communication between others.[35] The Fifth Circuit held that these big social media companies should be regulated as common carriers, which would empower the Texas Legislature to pass laws to ensure that the platforms do not discriminate against users.[36] These platforms, the Fifth Circuit noted, represent themselves as open to the public and essentially operate as "the modern public square."[37]

C. Holding

The Fifth Circuit held that social media companies are not "speaking" for the purposes of the First Amendment when they restrict users' ability to

27. NetChoice, LLC v. Paxton, 49 F.4th 439, 439 (5th Cir. 2022), *petition for cert. docketed*, No. 22-555 (U.S. Dec 19, 2022).
28. *Id.* at 445.
29. *Id.* at 455.
30. *Id.* at 439.
31. *Id.* at 448.
32. *Id.* at 459-60.
33. *Paxton*, 49 F.4th at 460.
34. *Id.* at 455.
35. *Id.* at 467.
36. *Id.* at 448.
37. *Id.* at 445 (quoting Packingham v. North Carolina, 582 U.S. 98, 107 (2017)).

post on their platforms.[38] Because of the dominant market share that these platforms have and the significant public interest in them, the Fifth Circuit held that they operate like common carriers more than newspapers exercising editorial judgment.[39] Thus, they do not have a constitutional right to censor what others say.[40] The Fifth Circuit reversed the district court's opinion and vacated the preliminary injunction.[41]

III. SUMMARY OF CIRCUIT SPLIT

In sum, the Eleventh Circuit struck down the Florida statute, arguing that social media companies are private actors engaging in constitutionally protected free speech when they make content moderation decisions.[42] The Fifth Circuit came to the opposite conclusion, finding that large social media companies are not engaging in speech when they censor users' content, and instead they operate more like common carriers (which means they are subject to nondiscrimination requirements).[43] The Supreme Court has delayed a decision about whether it will hear the cases, asking the U.S. Solicitor General to provide an opinion.[44] Whether the Supreme Court takes up the cases will have tremendous implications for this area of the law and how social media companies can moderate content on their platforms going forward.

38. *Id.* at 448.
39. *Paxton*, 49 F.4th at 494.
40. *Id.*
41. *Id.*
42. NetChoice, LLC v. Att'y Gen., 34 F.4th 1196, 1204 (11th Cir. 2022).
43. *Paxton*, 49 F.4th at 448.
44. *See* Lauren Feiner, *Supreme Court Punts on Texas and Florida Social Media Cases That Could Upend Platform Moderation*, CNBC (Jan. 23, 2023, 2:58 PM), https://www.cnbc.com/2023/01/23/supreme-court-punts-on-texas-and-florida-social-media-law-cases.html [https://perma.cc/NBA4-4HKG].

Twitter, Inc. v. Paxton

Jordyn Johnson

26 F.4TH 1119 (9TH CIR. 2022)

In 2021, after Twitter announced its decision to permanently ban former President Donald Trump, the Texas Office of the Attorney General ("OAG") served Twitter with a Civil Investigative Demand ("CID") asking the company to hand over documents concerning its content moderation decisions.[1] Twitter sued Ken Paxton in his official capacity as the Attorney General of Texas, maintaining that the CID was government retaliation against speech protected by the First Amendment.[2] The Northern District of California dismissed the case as unripe.[3] In response, Twitter filed an injunction pending appeal, which the District Court rejected, and a divided motions panel on the Ninth Circuit upheld the finding.[4] The Ninth Circuit then affirmed the motion to dismiss, finding that the case was prudentially unripe.[5]

I. BACKGROUND

Following the events at the United States Capitol on January 6, 2021, Twitter permanently banned former President Donald Trump from its platform.[6] In response, the Texas OAG asked Twitter to produce documents related to "its content moderation decisions" through a CID.[7] OAG said that it had been looking into Twitter's content moderation decisions for years because of citizen complaints.[8]

Consequently, Twitter sued Texas Attorney General Ken Paxton in the Northern District of California, arguing that "the act of sending the CID and the entire investigation were unlawful retaliation for its protected speech."[9] This was partly due to Paxton tweeting that Twitter was "closing conservative accounts" and promising that "[a]s AG, I will fight them with all I've got."[10] However, Twitter executives had previously claimed its content moderation policies were apolitical.[11] Twitter maintained that Paxton violated the

1. Twitter, Inc. v. Paxton (*Twitter I*), 26 F.4th 1119, 1121 (9th Cir.), *reh'g denied*, *amended & superseded en banc by* 56 F.4th 1170 (9th Cir. 2022).
2. *Id.*
3. *Id.* at 1122; *see also* Defendant's Motion to Dismiss at 2, Twitter, Inc. v. Paxton, No. 21-cv-01664-MMC (N.D. Cal. May 11, 2021), 2021 WL 5742108.
4. *Twitter I*, 26 F.4th at 1222.
5. *Id.*
6. *Id.* at 1221.
7. *Id.*
8. *Id.* at 1221-22.
9. *Id.* at 1122.
10. *Twitter I*, 26 F.4th at 1222..
11. *Id.*

company's First Amendment rights as a publisher because content moderation decisions were protected speech.[12] Further, it directed the District Court's attention to Paxton's tweets, claiming they showed his intent that serving Twitter with the CID was retaliation for banning President Trump.[13] Twitter asked the Northern District of California to prevent Paxton from enforcing the CID and find that the investigation violated the First Amendment.[14] Paxton challenged the case's ripeness, arguing that "pre-enforcement challenges to non-self-executing document requests are not ripe."[15] The District Court agreed and dismissed the case.[16] Twitter maintained that the case was ripe because it had suffered an injury through "chilled" speech and filed an injunction pending appeal.[17] A divided motions panel affirmed.[18] Twitter appealed to the United States Court of Appeals for the Ninth Circuit.[19]

II. ANALYSIS

"[R]ipeness is one of three justiciability requirements" courts use to determine whether a case can be decided.[20] Constitutional ripeness is defined as "whether the issues presented are definite and concrete, not hypothetical or abstract."[21] Prudential ripeness, on the other hand, requires courts "to 'evaluate both the fitness of the issues for judicial decision and the hardship to the parties of withholding court consideration.'"[22] The court focused on prudential ripeness in this case because it found it would be more difficult to determine constitutional ripeness.[23]

The "fit for decision" prong of the prudential ripeness doctrine requires courts to determine "if the issues raised are primarily legal, do not require further factual development, and the challenged action is final."[24] Twitter argued that it based its case on an act that had already occurred—that Paxton's intent in serving the CID was retaliatory.[25] However, the court thought the case turned on other questions, including whether Twitter's statements about its content moderation decisions were misleading.[26] Further, OAG had not alleged Twitter violated any law; it was merely investigating. Because this

12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. *Twitter I*, 26 F.4th at 1222.
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.*
21. *Id.* at 1123 (quoting Cal. Pro-Life Council, Inc. v. Getman, 328 F.3d 1088, 1094 n.2 (9th Cir. 2003)).
22. *Twitter I*, 26 F.4th at 1223 (quoting Ass'n of Irritated Residents v. EPA, 10 F.4th 937, 944 (9th Cir. 2021)).
23. *Id.* at 1124.
24. *Id.* at 1123 (quoting Skyline Wesleyan Church v. Cal. Dep't of Managed Health Care, 968 F.3d 738, 752 (9th Cir. 2020)).
25. *Id.* at 1124.
26. *Id.* at 1125.

question was not solely legal but rested on "further factual amplification," the court held it was unfit for decision.[27]

The hardship prong requires courts to consider if the action demands an immediate and meaningful "change in the plaintiffs' conduct of their affairs with serious penalties attached to noncompliance."[28] The Ninth Circuit found that Twitter did not have to comply with the CID, as OAG did not take any action that necessitated immediate compliance.[29] The Court held that if the action proceeded, OAG would have to present its argument in California federal court without the opportunity to research its own claims, undermining Texas's state sovereignty.[30]

Twitter next attempted to argue that the investigation was illegitimate because "editorial judgments" cannot be investigated.[31] To support its argument, Twitter relied on cases emphasizing the risks of government editorial oversight, such as *Miami Herald Publishing Company v. Tornillo*[32] and *Bullfrog Films, Inc. v. Wick*.[33] However, the court rejected applying those cases, as both relied on government regulations or statutes "which themselves required balance."[34] Here, Twitter made outright statements about balance, so the issue from those cases was absent.[35] Thus, Twitter's statements could be investigated like any other business'.[36]

Finally, Twitter asked the court to rely on four prior First Amendment cases—*Bantam Books v. Sullivan*, *White v. Lee*, *Wolfson v. Brammer*, and *Brodheim v. Cry*.[37] The Ninth Circuit first concluded that *Bantam Books* differed from the case at hand because (1) "it dealt with obscenity; (2) it addressed a state regulatory scheme that 'provide[d] no safeguards whatever against the suppression of nonobscene, and therefore constitutionally protected, matter;'[38] and (3) it did not address ripeness."[39] Next, the court found that Twitter incorrectly relied on *White* because there, "the plaintiffs had no opportunity to challenge any aspect of [an] investigation until formal charges were brought[.]"[40] Twitter could bring up a First Amendment defense if OAG tried to enforce the CID.[41] Further, *Wolfson*, was also not on point

---

27. *Id.* (quoting United States v. Lazarenko, 476 F.3d 642, 652 (9th Cir. 2007)).
28. *Twitter I*, 26 F.4th at 1123 (quoting Stormans, Inc. v. Selecky, 586 F.3d 1109, 1126 (9th Cir. 2009)).
29. *Id.* at 1125.
30. *Id.* at 1126.
31. *Id.*
32. Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 258 (1974) (holding that a statute forcing newspapers attacking the character of a political candidate to allow free space to a candidate to reply was an unconstitutional violation of the First Amendment).
33. *Twitter I*, 26 F.4th at 1126 (citing Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 510 (9th Cir. 1988) (finding unconstitutional regulations establishing specific criteria for evaluating eligibility for a certificate of international educational character)).
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.* at 1126-28.
38. *Id.* at 1126 (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963)).
39. *Twitter I*, at 1126-27.
40. *Id.* at 1128 (citing White v. Lee, 227 F.3d 1214, 1228 (9th Cir. 2000)).
41. *Id.*

because there was no investigation in that case, unlike here.[42] Finally, the court refused to apply *Brodheim* because it concerned "the disparity in power and control between prison officials and inmates, and such disparity is not present here."[43] Additionally, *Brodheim* did not address ripeness.[44]

Paxton maintained that the Ninth Circuit should apply *Reisman v. Caplin*, a case dealing with whether an accountant had to turn over documents requested by the IRS.[45] But in *Reisman*, "there had not yet been an injury," and the case did not mention ripeness.[46] On the contrary, Twitter, though insufficiently, alleged that it did suffer a constitutional injury.[47] Unlike in *Reisman*, Twitter could not avoid said "injury by challenging the document request later."[48]

Following this decision, Twitter filed a motion for reconsideration, which the Ninth Circuit denied en banc.[49]

III. CONCLUSION

The Ninth Circuit affirmed the District Court's order dismissing the case because the issues presented were not ripe for adjudication.[50] Twitter's claims neither showed that the CID chilled its speech by impeding its capacity to make content moderation decisions nor caused any other cognizable injury that an injunction would redress.[51]

42. *Id.* (citing Wolfson v. Brammer, 616 F.3d 1045, 1058 (9th Cir. 2010)).
43. *Id.* (citing Brodheim v. Cry, 584 F.3d 1262, 1266 (9th Cir. 2009)).
44. *Id.*
45. *Twitter I*, 26 F.4th at 1128 (citing Reisman v. Caplin, 375 U.S. 440, 443 (1964)).
46. *Id.* at 1129.
47. *Id.*
48. *Id.*
49. Twitter, Inc. v. Paxton (*Twitter II*), 56 F.4th 1170, 1172 (9th Cir. 2022) (en banc).
50. *Twitter I*, 26 F.4th at 1129.
51. *Id.*

Facebook, Inc. v. Noah Duguid, et al.

Sarah Lambert

141 S. CT. 1163 (2021)

In *Facebook v. Duguid,* the Supreme Court reversed the decision of the Ninth Circuit, holding that Facebook's notification system does not use the necessary "random or sequential number generator" technology to make The Telephone Consumer Protection Act of 1991 ("TCPA") applicable.[1] Petitioner Duguid's initial complaint alleged that Facebook's elective security measure giving users the option to receive text messages as a form of security alert violated the TCPA.[2] Facebook argued that their system did not fall under the TCPA since they did not use a random or sequential number generator.[3] The Court relied on methods of statutory interpretation to determine that a system must have a random or sequential number generator to be present to constitute a violation of the TCPA.[4]

I. BACKGROUND

The Telephone Consumer Protection Act of 1991 forbids abusive telemarketing practices, particularly by placing restrictions on communications made using an "automatic telephone dialing system."[5] Those who use an automatic telephone dialing system are identified as autodialers.[6] The TCPA further defines an "automatic telephone dialing system as "a piece of equipment with the capacity both 'to store or produce telephone numbers to be called, using a random or sequential number generator,' and to dial those numbers."[7] Here, petitioner Facebook, Inc. uses an elective security measure that gives users of their social media platform the option to receive text messages when there is a login attempt from a new device or browser.[8] Noah Duguid, the respondent, received such a text, which alerted him to a login in attempt on an account he had not created.[9] Duguid engaged in multiple attempts to stop the text messages, eventually bringing a putative class action against Facebook.[10]

1. Facebook, Inc. v. Duguid, 141 S. Ct. 1163, 1173 (2021).
2. *Id* at 1165.
3. *Id*.
4. *Id*.
5. *Id*.
6. *Id.*
7. 47 U.S.C. § 227(a)(1).
8. *See Facebook*, 141 S. Ct. at 1165.
9. *Id.*
10. *Id.*

Duguid's complaint alleges that Facebook violated the TCPA because their database had the ability to store numbers and distribute automated text messages.[11] In response, Facebook contended that the TCPA did not apply to their system because it did not use a "random or sequential number generator."[12] The Ninth Circuit agreed with Duguid, "holding that §227(a)(1) applies to a notification system like Facebook's that has the capacity to dial automatically stored numbers."[13]

Facebook appealed to the Supreme Court.[14] The issue was "whether the clause 'using a random or sequential number generator' in §227(a)(1)(A) modifies both of the two verbs that precede it ("store" and "produce"), as Facebook contends, or only the closest one ("produce"), as maintained by Duguid."[15]

Ultimately, the court decided that "to qualify as an 'automatic telephone dialing system' under the TCPA, a device must have the capacity either to store a telephone number using a random or sequential number generator, or to produce a telephone number using a random or sequential number generator."[16]

II. ANALYSIS

The Court came to their decision by looking at the text of the statute and the broader statutory context.[17] By reading the text of the statute in the most natural way and comparing that reading to other aspects of Section 227(a)(1)(A), the Court found that Facebook's view was most appropriate.[18] That conclusion was supported by three contentions regarding the modifying phrase "using a random or sequential number generator."[19] First, the court held the series qualifier canon applied to the "modifier at the end of a series to the entire series," which then applied the "using a random or sequential number generator" phrase to both the "store" and "produce" terms.[20] Facebook's program didn't produce phone numbers, and did not use any of the stored numbers in a random or sequential number generator, thus did not fall within the statute.[21] Second, the words "store" and "produce" were contained in an integrated clause, separated by the word "or."[22] Given the use of "or," "it would be odd to apply" the modifying phrase to those words individually or separately.[23] Finally, the modifying phrase is separated from

11. *Id.*
12. *Id.*
13. *Id.*
14. *See Facebook*, 141 S. Ct. at 1165.
15. *Id.*
16. *Id.*
17. *See id.* at 1165-66.
18. *Id.*
19. *Id.* at 1169.
20. *Facebook*, 141 S. Ct. at 1165.
21. *See id.* at 1169.
22. *Id.*
23. *Id.*

the antecedents by a comma, which suggests that the phrase should qualify each antecedent, instead of just one.[24]

Duguid maintains that the last antecedent rule would limit the modifying clause only to the phrase that it immediately follows.[25] However, Duguid's argument failed on two accounts. First, the last antecedent rule does not apply if the modifying clause follows an integrated list, as it does here with the "using a random or sequential number generator" phrase following the "store" or "produce" phrase.[26] Second, the phrase "telephone numbers to be called" is actually the last antecedent relevant to the modifying clause, not "produce."[27]

When analyzing the statute in context, the Court held that the TCPA was not intended to apply to equipment that does not have a random or sequential number generator.[28] Congress's intent in passing the statute was to mitigate the harmful effects of autodialer technology, such as unnecessary traffic on emergency lines.[29] Facebook's technology does not involve these concerns, and therefore, the Court opted for the interpretation that excluded its technology.[30] On the other hand, Duguid's interpretation would inappropriately extend the statute to any technology or equipment that is capable of storing and dialing telephone numbers.[31]

The Court also found Duguid's arguments concerning the text and context of the statute to be inappropriate.[32] Using Duguid's interpretation, the Court's decision would loop all equipment with the capacity to store and dial a phone number into the statute, which would include personal cell phones.[33] In addition, the distributive canon provides that "a series of antecedents and consequents should be distributed to one another based on how they most naturally relate in context."[34] Duguid argues that canon should be applied to this case, but the Court determined it was ill-suited because the number of consequents did not match up to the number of antecedents.[35] Duguid also attempted to use the TCPA's privacy protection goals, particularly focusing on consent, to aid his argument, but used too broad a reading of those goals in light of the choice to define autodialers precisely.[36] Lastly, Duguid argued that the statute should apply to updated, modern technology, as the number generator is likely to become obsolete or outdated, but that does not overrule Congress' chosen definition of autodialer.[37]

---

24. *Id.* at 1167.
25. *See id.* at 1170..
26. *See Facebook*, 141 S. Ct. at 1165-66 (citing Jama v. ICE, 543 U.S. 335, 344 (2005)).
27. *Id.* at 1170.
28. *See id.* at 1171.
29. *Id.*
30. *Id.* at 1172.
31. *Id.* at 1173.
32. *See Facebook*, 141 S. Ct. at 1172.
33. *See id.* at 1171.
34. *Id.* at 1166.
35. *See id.*
36. *See id.* at 1172.
37. *Id.*

III. CONCURRENCE (J. ALITO)

Justice Alito's concurring opinion agreed with the Court's reasoning and holding, but clarified that canons should not be used as a rule, but only when helpful to the statute's interpretation.[38] He also offered a different argument that would allow for series qualifiers to modify varying numbers of nouns or verbs in the list depending on the circumstance.[39] While it is unclear which is appropriate in the case, Justice Alito asserted that it is important to view the use of interpretive canons as a flexible, rather than inflexible rule.[40]

IV. CONCLUSION

Using both the text and context of the statute, the Court held that Facebook's notification system does not use the necessary "random or sequential number generator" technology to make the TCPA applicable.[41] The judgment of the Court of Appeals was reversed, and the case was remanded for further proceedings consistent with the opinion.[42]

38. *See Facebook*, 141 S. Ct. at 1173-75 (Alito, J., concurring).
39. *See id.* at 1174-75.
40. *Id.* at 1175.
41. *See id.* at 1173 (majority opinion).
42. *Id.*