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.