THE GOVERNMENT'S BEST-KEPT SECRET: HOW JAWBONING BECAME A LITTLE-KNOWN TOOL OF CISA IN THE DIGITAL AGE

Camryn Runyan*

* Camryn Runyan received a Bachelor of Arts in Political Science and Journalism from Baylor University. In 2025, she received a Juris Doctor from George Mason University Antonin Scalia Law School. Camryn would like to thank her friends and family for the invaluable guidance they so kindly provided during this process.

INTRODUCTION

The right to freedom of speech, which the First Amendment to the U.S. Constitution guarantees, fosters a "free trade in ideas."[1] Justice Holmes explained "that the best test of truth is the power of the thought to get itself accepted in the competition of the market."[2] This market provides access to novel and rudimentary ideas. If the government discreetly bars an idea from entering this market, however, the right to freedom of speech is weakened.

When proposing an amendment to guarantee free speech, James Madison invoked a theory of natural rights.[3] This theory suggests that individuals possess certain capacities that can be exercised without the government's involvement.[4] Madison insisted that the public should "not be deprived or abridged of their right to speak, to write, or to publish their sentiments."[5] Moreover, an individual retained this right to freedom of speech after the government's formation.[6]

The Founders embraced the right to freedom of speech as a means to protect against government censorship.[7] Madison believed that, in a republican government, the government should not have censorial power over the public.[8] From a broader perspective, John Stuart Mill explained there are some "departments of human life" that require "space in human existence . . . entrenched around, and sacred

[1] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).
[2] *Id.*
[3] David S. Bogen, *The Origins of Freedom of Speech and Press*, 42 MD. L. REV. 429, 451 (1983).
[4] Jud Campbell, *Natural Rights and the First Amendment*, 127 YALE L.J. 246, 268 (2017).
[5] 1 ANNALS OF CONG. 451 (1789) (Joseph Gales ed., 1834).
[6] Jonathan Turley, *Harm and Hegemony: The Decline of Free Speech in the United States*, 45 HARV. J.L. & PUB. POL'Y 571, 582 (2022).
[7] *See id.* at 613.
[8] *See* 4 ANNALS OF CONG. 934 (1794).

from authoritative intrusion."[9] Free speech is one such department.[10] Yet today's age of information and technology poses a dilemma. The "space in human existence" that Mill described[11] is no longer only physical.[12] It now includes the internet and social media platforms.[13] Because of this development, governmental "attempts to check the expression of opinions"[14] are more difficult to identify and evaluate.

Today's dilemma "is different from any prior period due to new technological, political, and economic pressures on the exercise of free speech."[15] Technology's broad accessibility and affordability has allowed more people to spread more speech.[16] This free speech free-for-all has also led to an increase in demand for censorship.[17] While questions regarding the scope of the First Amendment remain open, Professor Jonathan Turley argues this "growing support for censorship" presents "the greatest threat to free speech today."[18]

This Comment explores the government's role in monitoring speech on social media during the 2020 election season. Part I specifically examines the U.S. Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency's ("CISA") interactions with social media platforms and third-party intermediaries. Part II analyzes the First Amendment case law that governs this conduct. Part III confirms that Congress is best suited to

---

[9] JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY WITH SOME OF THEIR APPLICATIONS TO SOCIAL PHILOSOPHY 942-43 (W.J. Ashley ed., Longmans, Green, & Co. 7th ed. 1909) (1848).
[10] Turley, *supra* note 7, at 641 (citing JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY (1848), *reprinted in* 3 THE COLLECTED WORKS OF JOHN STUART MILL 938 (J.M. Robson, ed., 1965).
[11] MILL, *supra* note 9, at 943.
[12] Turley, *supra* note 6, at 641.
[13] *Id.*
[14] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).
[15] Turley, *supra* note 7, at 571.
[16] *See* Will Duffield, *Jawboning Against Speech: How Government Bullying Shapes the Rules of Social Media*, CATO INST.: POL'Y ANALYSIS NO. 934, at 4 (Sept. 12, 2022), https://www.cato.org/sites/cato.org/files/2022-09/PA_934.pdf.
[17] *See id.*
[18] Turley, *supra* note 7, at 572.

address this issue and discusses proposed, as well as potential, legislative considerations.

I. JAWBONING: A FORM OF CENSORSHIP BY PROXY

One foundational principle governs this discussion—the government "cannot do indirectly what [it] is barred from doing directly."[19] Thus, the government cannot sidestep the First Amendment by using a private actor to suppress speech it does not like.[20] "Jawboning" is used to describe this form of "censorship by proxy."[21] In light of today's abundance of digital speech,[22] the opportunity for government jawboning is especially great and must be carefully examined.

A. *The Rise of Jawboning*

Jawboning is defined as "the use of official speech to inappropriately compel private action."[23] In practice, the government dissuades a private intermediary, such as a book distributor or social media platform, from carrying certain speech.[24] Instead of attacking the speaker, the government disrupts the "chain of connections" by using "private actors within the chain as proxy censors to control the flow of information."[25] Outsourcing this pressure campaign to a private actor benefits the government since the actor largely bears the costs associated with policing speech.[26]

---

[19] Nat'l Rifle Ass'n of Am. v. Vullo, 602 U.S. 175, 190 (2024) (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 67-69 (1963)).
[20] *Id.*
[21] Devin Watkins, *CEI Welcomes Supreme Court Review of Censorship 'Jawboning' Case*, COMPETITIVE ENTER. INST. (Nov. 3, 2023), https://cei.org/news_releases/cei-welcomes-supreme-court-review-of-censorship-jawboning-case/.
[22] *See* Duffield, *supra* note 16, at 4.
[23] *Id.* at 2.
[24] *See id.*
[25] Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 14 (2006).
[26] *Id.* at 27.

Historically, the government attempted to jawbone the economy.[27] Jawboning entered "the political lexicon when President Kennedy sought to restrain prices and wages in the steel industry."[28] During his presidency, "an overheating economy gradually pushed up prices."[29] In response to this event, President Kennedy tried to prevent steel producers from increasing prices by threatening to take legal action and scrap government contracts.[30] While the economy was the target of jawboning during this period, the government would later target speech.[31]

Today, the government has successfully normalized efforts to increase its involvement online, especially with social media platforms, by adopting a functionalist theory of speech.[32] Generally, functionalism suggests that "society is in a state of balance and kept that way through the function of society's component parts."[33] The value of the targeted speech is a key consideration under a functionalist theory of speech.[34] Censorship is justified by stressing the harm that low-value speech may have on public discourse if it is allowed to remain online.[35] If this view is embraced, "speech denial can become merely a matter of perspective."[36]

Censorship by proxy is an especially effective government tool, when applied to the internet and social media platforms, because it often occurs behind closed doors.[37] Generally, the public is unaware

---

[27] *See* Christopher Frey, *Bad to the [Jaw]Bone: How Courts Should Approach First Amendment Jawboning Challenges*, 55 SETON HALL L. REV. 205, 209-10 (2024).
[28] Paul R. Verkuil, *Jawboning Administrative Agencies: Ex Parte Contacts by the White House*, 80 COLUM. L. REV. 943, 943 n.1 (1980).
[29] Jeanna Smialek & Ben Casselman, *A Great Inflation Redux? Economists Point to Big Differences.*, N.Y. TIMES (Oct. 11, 2021), https://www.nytimes.com/2021/07/08/business/economy/inflation-redux.html.
[30] Frey, *supra* note 27, at 209-10; *see* Duffield, *supra* note 16, at 2.
[31] Frey, *supra* note 27, at 210.
[32] *See* Turley, *supra* note 7, at 610.
[33] RON HAMMOND ET AL., *Social Theories*, *in* INTRODUCTION TO SOCIOLOGY (2020), https://freesociologybooks.com/Introduction_To_Sociology/03_Social_Theories.php.
[34] *See* Turley, *supra* note 6, at 610.
[35] *See id.*
[36] *Id.* at 606.
[37] *See* Kreimer, *supra* note 25, at 28.

of the government's involvement, so it becomes "not just censorship, but unaccountable censorship."[38] Typically, neither the author nor the reader knows that a particular post was removed.[39] Users are not informed that the government was involved in the platform's review of the user's speech.[40] After all, "[p]rivate discretion is often less visible and less procedurally regular than public sanction."[41] Without transparency, a user, as well as the public at large, remains unapprised of government conduct.

While courts have encountered "jawboning in the past, it has been given a new life in the internet age."[42] As more people joined the "[d]igital [p]ublic [s]quare,"[43] the government shifted its jawboning efforts to social media platforms.[44] In light of this development, "questions surrounding the limits of speech-related jawboning have become particularly salient."[45] Generally, courts resolve jawboning cases by differentiating between constitutional persuasion and unconstitutional coercion, "whereby jawboning effectively becomes censorship."[46] However, the line between persuasion and coercion is blurry—especially in the digital age.[47]

B. *A Modern Case Study: CISA*

The "contemporary revival of jawboning" occurred after the 2016 presidential election.[48] CISA was established to address

[38] *See* Duffield, *supra* note 16, at 7.
[39] *See* Kreimer, *supra* note 25, at 28.
[40] *See* Duffield, *supra* note 16, at 7.
[41] Kreimer, *supra* note 25, at 65.
[42] Duffield, *supra* note 16, at 2.
[43] *See generally* Adeline Von Drehle, *Censorship and the Digital Public Square*, REALCLEAR POL. (Mar. 20, 2024), https://www.realclearpolitics.com/articles/2024/03/20/censorship_and_the_digital_public_square_150675.html.
[44] Frey, *supra* note 27, at 206.
[45] *Id.*
[46] *Id.* at 207.
[47] *See* Duffield, *supra* note 16, at 2.
[48] *Id.* at 9.

lawmakers' increasing concerns "about possible cyberattacks."[49] It was believed this new agency would "streamline federal cybersecurity efforts, encourage industry to improve vulnerable systems and help safeguard critical infrastructure."[50] But in early 2017, outgoing DHS Secretary Jeh Johnson expanded the definition of critical infrastructure to include election infrastructure.[51] The meaning of critical infrastructure came to encompass meta-physical items.[52] It changed "from physical things like satellites and dams and federal buildings to events like elections or public health campaigns."[53]

While CISA has struggled to identify a cohesive strategy to address this broadened mission space,[54] one of its initial moves appears to have granted it "long-arm jurisdiction [over] social media" and domestic speech.[55] In 2018, DHS formed the Countering Foreign Influence Task Force ("CFITF") within CISA's Election Security Initiative ("ESI").[56] CFITF was established "to focus on election

[49] *See* Suzanne Smalley et al., *Insiders Worry CISA Is Too Distracted from Critical Cyber Mission*, CYBERSCOOP (Dec. 22, 2022), https://cyberscoop.com/cisa-dhs-easterly-cyber-mission/.

[50] *Id.*

[51] Press Release, Jeh Johnson, Sec'y, U.S. Dep't of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[52] *See* Mike Benz, *DHS Censorship Agency Had Strange First Mission: Banning Speech that Casts Doubt on 'Red Mirage, Blue Shift' Election Events*, FOUND. FOR FREEDOM ONLINE (Nov. 9, 2022), https://foundationforfreedomonline.com/dhs-censorship-agency-had-strange-first-mission-banning-speech-that-casts-doubt-on-red-mirage-blue-shift-election-events/.

[53] *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Fed. Gov't of the H. Comm. on the Judiciary*, 118th Cong. 43 (2023) [hereinafter *Hearing on Weaponization*] (prepared statement of Michael Shellenberger, Journalist).

[54] *See* Smalley et al., *supra* note 49.

[55] *See* Mike Benz, *DHS Scrubs YouTube Channel of Infamous Censorship Video Encouraging People to Report Family Members for "Disinformation,"* FOUND. FOR FREEDOM ONLINE (Nov. 28, 2023), https://foundationforfreedomonline.com/dhs-website-uncle-steve-family-members/.

[56] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, #PROTECT2020 STRATEGIC PLAN 4 (2020), https://web.archive.org/web/20220316030323/https://www.cisa.gov/sites/default/files/publications/ESI_Strategic_Plan_FINAL_2-7-20_508.pdf.

infrastructure disinformation."[57] In early 2021, CISA modified the CFITF to gain greater flexibility over general misinformation, disinformation, and malinformation ("MDM").[58] From this transition, CISA assembled an MDM team of fifteen staff members to "focus[] on disinformation activities targeting elections and critical infrastructure."[59]

Three definitions guided CISA's work in this space.[60] CISA defined misinformation as "false [information that was] not created or shared with the intention of causing harm."[61] Conversely, disinformation encompassed information that was "deliberately created to mislead, harm, or manipulate a person, social group, organization, or country."[62] Lastly, CISA defined malinformation as information "based on fact, but used out of context to mislead, harm, or manipulate."[63] By this definition, the government could deem a fact objectionable because it was not supplemented with a sufficient amount of context.[64]

According to CISA, "[d]isinformation actors use a variety of tactics to" manipulate minds, spur action, and inflict harm.[65] These

[57] OFF. OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-22-58, DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS 5 (2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf.
[58] *See id.* at 6-7.
[59] *Id.* at 7.
[60] *See Foreign Influence Operations and Disinformation*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY: ELECTION SECURITY, https://web.archive.org/web/20240719165923/https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation#expand.
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *See* U.S. H.R. COMM. ON THE JUDICIARY & THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS 10 (2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf.
[65] *See Tactics of Disinformation*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://web.archive.org/web/20221019010737/https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf.

tactics also threaten critical infrastructure.[66] CISA identified, for example, the amplification of conspiracy theories as one disinformation tactic.[67] Because conspiracy theories can change an individual's worldview, CISA encouraged organizations to practice "proactive resilience building . . . to prevent conspiratorial thinking from taking hold."[68] While MDM tactics were not a novel development, CISA maintained that the emergence of technology generated "new vectors for exploitation."[69]

More aggressive efforts to fight disinformation materialized during the 2020 election season and COVID-19 pandemic.[70] While speaking at a conference in 2021, CISA Director Jen Easterly said, "One could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important."[71] Easterly also announced she would be strengthening CISA's misinformation and disinformation team.[72] Ultimately, CISA's role was based on mitigating the risks associated with foreign MDM,[73] and because those risks, according to CISA, only increased in recent years,[74] CISA took action.

---

[66] *Id.*
[67] *See id.*
[68] *Id.*
[69] *See CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 2022) [hereinafter *CISA Insights*], https://web.archive.org/web/20240531143841/https://www.cisa.gov/sites/default/files/2023-09/Preparing%20for%20and%20Mitigating%20Foreign%20Influence%20Operations%20Targeting%20Critical%20Infrastructure.pdf.
[70] *See* Ken Klippenstein & Lee Fang, *Truth Cops: Leaked Documents Outline DHS's Plans to Police Disinformation*, THE INTERCEPT (Oct. 31, 2022, 5:00 AM), https://theintercept.com/2022/10/31/social-media-disinformation-dhs/.
[71] Maggie Miller, *Cyber Agency Beefing Up Disinformation, Misinformation Team*, THE HILL (Nov. 10, 2021, 2:52 PM), https://thehill.com/policy/cybersecurity/580990-cyber-agency-beefing-up-%20disinformation-misinformation-team/.
[72] *Id.*
[73] *See Foreign Influence Operations and Disinformation*, *supra* note 60.
[74] *See CISA Insights*, *supra* note 69.

1. CISA's Influence via Switchboarding

In 2018, CISA debuted a "switchboarding" operation.[75] According to CISA, CISA's "MDM team serve[d] as a switchboard for routing disinformation concerns to appropriate social media platforms."[76] In practice, if a state or local election official identified a social media post or account that resembled disinformation, the official could forward that information to CISA.[77] CISA then sent the information to social media platforms.[78] These communications "included disclaimers that [CISA] would not take any favorable or unfavorable action toward the companies based on how they used the information."[79] During this operation, officials did not "assess[] whether the content came from foreign or domestic speakers."[80] After switchboarding a post or account, CISA could follow up with platforms to check the status of the information submitted.[81]

[75] Response to Applicants' Third Supplemental Memorandum Regarding Application for a Stay of Injunction at 5, Murthy v. Missouri, 603 U.S. 43 (2024) (No. 23A243) [hereinafter Response to Application for Stay of Injunction].
[76] *Mis, Dis, Malinformation*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://web.archive.org/web/20210501230502/http://cisa.gov/mdm (choose "Bridging Election Stakeholders and Social Media" from dropdown).
[77] Missouri v. Biden, 680 F. Supp. 3d 630, 679 (W.D. La.), *aff'd in part*, *rev'd in part*, *vacated in part*, 83 F.4th 350 (5th Cir. 2023), *rev'd sub nom.* Murthy v. Missouri, 603 U.S. 43 (2024).
[78] *Id.*
[79] Derek B. Johnson, *CISA Moves Away from Trying to Influence Content Moderation Decisions on Election Disinformation*, CYBERSCOOP (Sept. 3, 2024), https://cyberscoop.com/cisa-moves-away-from-trying-to-influence-content-moderation-decisions-on-election-disinformation/.
[80] *Censorship Laundering: How the U.S. Department of Homeland Security Enables the Silencing of Dissent: Hearing Before the Subcomm. on Oversight, Investigations, and Accountability of the H. Comm. on Homeland Sec.*, 118th Cong. 16 (2023) [hereinafter *Censorship Laundering*] (prepared statement of Benjamin Weingarten, Investigative Journalist and Columnist).
[81] *See* U.S. H.R. COMM. ON THE JUDICIARY & THE SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, 118TH CONG., THE WEAPONIZATION OF "DISINFORMATION" PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS' POLITICAL SPEECH 18 (2023) [hereinafter UNIVERSITY REPORT], https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/EIP_Jira-Ticket-Staff-Report-11-7-23-Clean.pdf (In one email exchange between CISA and Twitter, a Twitter employee

This practice intensified during the 2020 election.[82] At the time, CISA characterized switchboarding as a natural extension of its election security efforts.[83] According to an archived capture of CISA's MDM webpage, CISA publicly advertised that it had "expanded the breadth of reporting to include" more officials and more platforms.[84] This allowed CISA to "leverage[] the rapport the MDM team ha[d] with . . . social media platforms" to ultimately function as a switchboard for directing disinformation.[85] Despite CISA's initial efforts to switchboard content, CISA discounted the operation in 2022.[86]

2. CISA's Influence via Third Parties

CISA also partnered with a third party to better "understand rumors and disinformation around the 2020 election."[87] In the summer of 2020, the Election Integrity Partnership ("EIP") was formed "as a coalition of research entities who . . . focus[ed] on supporting real-time information exchange between the research community, election officials, government agencies, civil society organizations, and social media platforms."[88] This partnership included the Stanford University Internet Observatory ("SIO"), the University of Washington Center for an Informed Public, the Atlantic Council Digital Forensic Research Lab ("DFRLab"), and Graphika.[89] Because no federal agency, including CISA, focused on domestic

confirmed that Twitter would ask a team to review a misinformation incident. Four days later, a CISA official followed up: "Checking in to see if there is anything that can be shared in regards to this reported incident.").

[82] *See* Response to Application for Stay of Injunction, *supra* note 75, at 5.

[83] *See Mis, Dis, Malinformation*, *supra* note 76.

[84] *Id.*

[85] *Id.*

[86] *See* Johnson, *supra* note 79.

[87] *A Statement from the Election Integrity Partnership*, ELECTION INTEGRITY P'SHIP (Oct. 5, 2022), https://www.eipartnership.net/blog/a-statement-from-the-election-integrity-partnership.

[88] ELECTION INTEGRITY P'SHIP, THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION 2 (2021), https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf.

[89] *Id.*

misinformation relating to elections, these organizations saw "a critical gap for non-governmental entities to fill."[90]

CISA appeared to be a reliable partner to the EIP during its development.[91] Before the EIP was officially announced, CISA pledged to maintain "open lines of communication" with SIO representatives.[92] In adherence with this pledge, CISA remained in contact with the EIP in the lead-up to the 2020 election.[93] At the outset, the director of the SIO notified one social media platform of the EIP's formation and explained that it would operate as "a one-stop shop for local election officials, DHS, and voter protection organizations to report potential disinformation . . . to investigate and to refer to the appropriate platforms."[94] This explanation indicated the CISA/EIP partnership would extend beyond the EIP's launch.

In 2020, the EIP began to manage speech items and communicate with social media platforms through the commercial tool, Jira,[95] which was used as "an internal ticketing workflow management system."[96] Jira allowed internal analysts and external actors to simultaneously participate in this operation.[97] If an analyst identified a potential item of misinformation, the analyst could generate a ticket on that item.[98] Alternatively, if an external actor emailed a tip line, the system "automatically generate[d] a ticket."[99] A ticket could address "one piece of content, an idea or narrative, or hundreds of URLs pulled in a data dump."[100] Through this system, the

[90] *Id.* at v.
[91] *See* UNIVERSITY REPORT, *supra* note 81, at 35-37.
[92] *See id.* at 36-37.
[93] *See id.* at 44-46.
[94] *See id.* at 38; *see also Alex Stamos,* STAN. UNIV. INTERNET OBSERVATORY CYBER POL'Y CTR., https://cyber.fsi.stanford.edu/io/people/alex-stamos (last visited Mar. 30, 2025) (identifying Alex Stamos as the director of the SIO).
[95] *See* UNIVERSITY REPORT, *supra* note 81, at 54.
[96] *See* ELECTION INTEGRITY P'SHIP, *supra* note 88, at 8, 24 n.6.
[97] *See id.*
[98] *See id.* at 8.
[99] *Id.*
[100] *Id.* at 9.

EIP could collect external tips and internally track its progress monitoring speech.[101]

The EIP also examined tickets based on "delegitimization."[102] The EIP defined delegitimization as "content aiming to delegitimize election results on the basis of false or misleading claims."[103] Analyzing tickets under this broad category allowed the EIP to inspect even more speech.[104] Therefore, if a user posted election-related misinformation, that speech could also be flagged because it could sow doubt on the results.[105] In total, seventy-two percent of tickets that the EIP internally processed "were related to delegitimization of the election."[106]

Once a ticket was generated, the EIP's work was underway. First, an analyst reviewed the ticket and could also add a comment.[107] After this preliminary review, a manager determined whether to share the ticket with the relevant platform or stakeholder.[108] In this system, a tagged actor could communicate with other actors about a ticket.[109] Despite describing itself as a cross-disciplinary research program,[110] the EIP appeared to use "recommend," and other similar terms, more than 100 times in the comments of ticket entries.[111] Ultimately, thirty-five percent of the URLs the EIP shared with social media platforms

---

[101] *See* Ben Weingarten, *Documents Shed New Light on Feds' Collusion with Private Actors to Police Speech on Social Media*, REALCLEAR INVESTIGATIONS (Nov. 6, 2023), https://www.realclearinvestigations.com/articles/2023/11/06/documents_shed_new_light_on_feds_collusion_with_private_actors_to_police_speech_on_social_media_990672.html?mobile_redirect=false.

[102] *See* ELECTION INTEGRITY P'SHIP, *supra* note 88, at vi.

[103] *See id.*

[104] *See Hearing on Weaponization*, *supra* note 53, at 48 (prepared statement of Michael Shellenberger, Journalist).

[105] *See id.*

[106] ELECTION INTEGRITY P'SHIP, *supra* note 88, at vi, 27.

[107] Brief for Representative Jim Jordan and 44 Other Members of Congress as *Amici Curiae* Supporting Respondents at 28, Murthy v. Missouri, 603 U.S. 43 (2024) (No. 23-411).

[108] *Id.*; *see* Weingarten, *supra* note 101.

[109] Weingarten, *supra* note 101.

[110] *See* Brief for Stanford University as *Amicus Curiae* Supporting Petitioners at 4, Murthy v. Missouri, 603 U.S. 43 (2024) (No. 23-411) [hereinafter Brief for Stanford University].

[111] Weingarten, *supra* note 101.

"were either labeled, removed, or soft blocked."[112] These data points indicate the EIP was more than "a passive research effort."[113]

Determining the scope of CISA's involvement in the EIP's operation is a fact-intensive inquiry and does not produce a unanimous conclusion. According to the SIO, CISA did not have any involvement in the EIP's formation and instead maintained an "arms-length relationship" with the SIO.[114] During its operation, the SIO claims the EIP spent "very little" time communicating with the government or social media platforms.[115] While it is difficult to pinpoint CISA's exact role in the EIP's affairs, CISA's conduct during this phase naturally raises questions about the application of government jawboning and the First Amendment, especially in today's digital age.

CISA knew, to some degree, "what was being reported to the EIP."[116] The Center for Internet Security ("CIS"), a nonprofit organization partly funded by CISA,[117] operated the Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC")[118] and forwarded various misinformation items to the EIP and CISA.[119] Because "CISA . . . was [routinely] copied on emails from CIS to the EIP," CISA knew which items were being sent to the EIP.[120] In some instances, CIS included the relevant social media platform in the email chain when forwarding an item to the EIP and CISA.[121] Through

[112] ELECTION INTEGRITY P'SHIP, *supra* note 88, at 27.
[113] Weingarten, *supra* note 101.
[114] *Stanford Files Amicus Brief in Murthy v. Missouri Pending Before U.S. Supreme Court*, STAN. UNIV. INTERNET OBSERVATORY CYBER POL'Y CTR. (Mar. 5, 2024), https://cyber.fsi.stanford.edu/io/news/update-amicus-sio-2024.
[115] *Id.*
[116] *See* UNIVERSITY REPORT, *supra* note 81, at 55.
[117] *Who Is CIS?*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/insights/blog/who-is-cis (last visited Mar. 30, 2025).
[118] *See* UNIVERSITY REPORT, *supra* note 81, at 21-22.
[119] *See id.* at 55.
[120] *See id.*
[121] *See id.* at 10, 57. For example, in one email to the EIP and CISA, CIS wrote, "Brian [the leader of the CFITF] and EIP—we have included Facebook in this report." *Id.* CIS copied two Facebook employees to the email. *Id.* at 57.

these routine email chains, social media platforms became more aware of CISA's involvement in this flagging operation.[122]

Additionally, CISA was actively mentioned and "tagged" on Jira.[123] Based on the SIO director's statement that CISA was on Jira[124] and a CISA official's use of a ticket's EIP-specific code,[125] CISA, at the very least, was not completely barred from viewing Jira activity. Without some level of access to information stored on Jira, it would be difficult to reference a ticket's EIP-specific code. Furthermore, Jira shared certain information with CISA.[126] Overall, examining the scope of CISA's involvement in these switchboarding operations provides a helpful case study on the application of government jawboning in the digital age. Determining whether that involvement implicates the First Amendment will be the focus of Part II.

II. JAWBONING AND THE FIRST AMENDMENT

Three foundational principles govern issues involving government jawboning of speech.[127] First, the government cannot suppress speech "because of its message, its ideas, its subject matter, or its content."[128] Second, the government cannot compel a private actor into doing what the government is constitutionally barred from doing.[129] Third, the First Amendment "does not regulate government

---

[122] *See id.* at 57.
[123] *Id.* at 91.
[124] *See* UNIVERSITY REPORT, *supra* note 81, at 91 (discussing one email to a Reddit employee in which the SIO director encouraged Reddit to participate in Jira by writing, "It would be great if we could get somebody from Reddit on the JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, [and] CISA . . . .").
[125] *Id.* at 59. In one email to Twitter employees, a CISA official referred to a ticket's EIP-specific code when switchboarding an item. *Id.* To assist the employees, the official wrote, "Please see below reporting from Connecticut election officials. The ticket is also tagged EIP-572." *Id.*
[126] *See id.* at 90. For example, in one email to a Facebook employee, Jira stated that information on ticket "EIP-833," regarding absentee ballots, was "shared with . . . CISA CFITF." *Id.*
[127] *See* Frey, *supra* note 27, at 212-16.
[128] Police Dep't Chi. v. Mosley, 408 U.S. 92, 95 (1972).
[129] Norwood v. Harrison, 413 U.S. 455, 465 (1973) (quoting Lee v. Macon Cnty. Bd. of Educ., 267 F. Supp. 458, 475-76 (M.D. Ala. 1967)).

speech."[130] This means, the government is free "to engage in much persuasion about speech."[131] However, the government cannot use this power to coercively censor speech.[132]

The Supreme Court previously explored the bounds of these First Amendment principles during the Warren Court.[133] And while this issue made its way back to the Court in 2024,[134] the Court ultimately declined to "provide guidance on what constitutes impermissible government coercion of social media platforms."[135]

A. *Guiding Precedent*

The legal landscape that governs jawboning is fractured.[136] Generally, courts apply two historical Supreme Court cases when resolving disputes over jawboning.[137] These cases, discussed below, "employ markedly different approaches to the question of when government efforts to encourage or pressure private parties into doing, or not doing, something implicate the First Amendment."[138] More recently, the Court decided a case involving government

[130] Pleasant Grove City v. Summum, 555 U.S. 460, 467 (2009).
[131] Philip Hamburger, *Courting Censorship*, 4 J. FREE SPEECH L. 195, 201 (2023).
[132] Frey, *supra* note 27, at 216.
[133] *See, e.g.*, Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 65-67 (1963).
[134] *See* Murthy v. Missouri, 603 U.S. 43, 54 (2024).
[135] David Greene, *Supreme Court Dodges Key Question in Murthy v. Missouri and Dismisses Case for Failing to Connect the Government's Communication to Specific Platform Moderation*, ELEC. FRONTIER FOUND. (July 22, 2024), https://www.eff.org/deeplinks/2024/07/supreme-court-dodges-key-question-murthy-v-missouri-and-dismisses-case-failing.
[136] *See* Mayze Teitler, *Doctrinal Disarray*, KNIGHT FIRST AMEND. INST. AT COLUMBIA UNIV.: JAWBONING (Mar. 15, 2024), https://knightcolumbia.org/blog/doctrinal-disarray.
[137] *See* Genevieve Lakier, *Informal Government Coercion and the Problem of "Jawboning,"* LAWFARE (July 26, 2021, 3:52 PM), https://www.lawfaremedia.org/article/informal-government-coercion-and-problem-jawboning.
[138] *Id.*

coercion of financial entities but "the reach of the opinion [to other contexts remains] uncertain."[139]

In *Bantam Books, Inc. v. Sullivan*, the Court found that a state commission unconstitutionally censored a distributor's printed material when it repeatedly notified the distributor that his material was not appropriate for children.[140] By thanking the distributor in advance and reminding him of possible prosecution, the commission "acted as an agency not to advise but to suppress."[141] These orders, disguised as notices, forced the distributor to stop circulating the material.[142] Accordingly, the government could not use its authority to bully a private actor into suppressing another person's speech in an effort to avoid threatened consequences.[143] This remains true "even if the threats the government makes are implicit, attenuated and ultimately empty."[144]

Almost two decades later, the Court revisited this question with a different approach in *Blum v. Yaretsky*.[145] There, the Court held that a private actor's decision can be attributed to the government if the government "exercised coercive power or . . . provided such significant encouragement, either overt or covert, that the choice must in law be deemed . . . that of the State."[146] A privately-owned nursing home's decision to release or transfer an admitted patient does not turn into government action when the government merely adjusts the patient's benefits in response to the decision.[147] The Court found that the decision-making process centered on independent medical

[139] Peter Shane, *NRA Ruling Doesn't Clarify Boundaries of Official Censorship*, BLOOMBERG L. (June 5, 2024, 4:31 AM), https://news.bloomberglaw.com/us-law-week/nra-ruling-doesnt-clarify-boundaries-of-official-censorship.
[140] *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 61, 72 (1963).
[141] *See id.* at 62, 72.
[142] *Id.* at 68.
[143] *See* Lakier, *supra* note 137.
[144] *Id.*
[145] *See generally* Blum v. Yaretsky, 457 U.S. 991 (1982).
[146] *Id.* at 1004.
[147] *Id.* at 1010.

judgment.[148] To trigger the Constitution, the government must be responsible for the private actor's conduct.[149]

B. *Recent Cases*

In 2024, the Court faced this issue again when it applied *Bantam Books* to the facts in *National Rifle Association of America v. Vullo*.[150] Based on the allegations in the complaint, the Court held that a New York Department of Financial Services ("DFS") official "violated the First Amendment by coercing DFS-regulated entities into disassociating with the NRA in order to punish or suppress the NRA's gun-promotion advocacy."[151] The NRA initially partnered with DFS-regulated entities for insurance purposes.[152] The official, meanwhile, coerced Lloyd's, an insurance marketplace,[153] when she said she would disregard prior infractions if Lloyd's ended its practices with the NRA and other similar organizations.[154] And like the distributor in *Bantam Books*, Lloyd's complied.[155] The Court concluded that this decision "d[id] not break new ground."[156] It simply reaffirmed the principle set out in *Bantam Books*—the government cannot coerce a private actor into suppressing disfavored speech.[157]

Because the Supreme Court's initial guidance left much to interpretation, the framework that lower courts applied when examining jawboning varied "from case to case."[158] The Ninth Circuit, for example, explained that "government officials do not violate the First Amendment when they request that a private intermediary not carry a third party's speech so long as the officials do not threaten

[148] *See id.* at 1008.
[149] *See id.* at 1004.
[150] *See generally* Nat'l Rifle Ass'n of Am. v. Vullo, 602 U.S. 175 (2024).
[151] *Id.* at 191.
[152] *See id.* at 181.
[153] *Welcome to Lloyd's*, LLOYD'S, https://www.lloyds.com/about-lloyds (last visited Mar. 30, 2025).
[154] *Vullo*, 602 U.S. at 192-93.
[155] *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 63, 68 (1963); *id.* at 193.
[156] *Vullo*, 602 U.S. at 197.
[157] *Id.* at 190,197 (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963)).
[158] *See* Lakier, *supra* note 137.

adverse consequences if the intermediary refuses to comply."[159] Accordingly, the Ninth Circuit held that the California Office of Elections Cybersecurity ("OEC") did not coerce a private actor when the OEC flagged a user's post and requested that the social media platform remove it.[160] Simple persuasion—like the government's conduct in this case—is a form of "permissible government speech."[161]

In a separate decision, the Ninth Circuit held that U.S. Senator Elizabeth Warren did not unconstitutionally coerce Amazon into suppressing a bestselling book's distribution when she sent a letter to the CEO that mentioned Amazon's possible participation in "peddling misinformation about COVID-19 vaccines and treatments" and "potentially unlawful" conduct.[162] Had Senator Warren included a statement regarding the possibility of adverse consequences if Amazon failed to comply with her request, the letter could have crossed into the zone of unconstitutional coercion.[163] But the letter contained no such statement.[164] Ultimately, the Ninth Circuit determined that "[t]he words on the page and the tone of the interaction" indicated the letter was used as a vehicle to persuade, not to coerce.[165]

In contrast, the Seventh Circuit held that a sheriff was coercive when he requested that credit card companies restrict cardholders from purchasing ads on Backpage, a classified advertising website that published adult ads.[166] The sheriff implied the companies could face prosecution for allowing cardholders to purchase ads "that promote unlawful sexual activity."[167] Facing potential adverse government action, the companies obliged.[168]

---

[159] O'Handley v. Weber, 62 F.4th 1145, 1158 (9th Cir. 2023).
[160] *See id.* at 1157-58.
[161] *See id.* at 1163.
[162] *See* Kennedy v. Warren, 66 F.4th 1199, 1204-05, 1207-08 (9th Cir. 2023).
[163] *See id.* at 1211.
[164] *See id.*
[165] *Id.* at 1209-10.
[166] Backpage.com, LLC v. Dart, 807 F.3d 229, 230-31, 233 (7th Cir. 2015).
[167] *See id.* at 232.
[168] *See id.*

C. *Varied Perspectives on CISA*

Engaging in a fact-intensive inquiry to distinguish between persuasion and coercion[169] can produce perspective-driven, subjective interpretations of government speech.[170] As a consequence of this ambiguity, determining whether CISA coerced social media platforms to suppress certain speech on CISA's behalf[171] is not a simple task. This inquiry, as demonstrated below, contains two competing perspectives.

From one perspective, CISA lawfully spoke as a concerned government agency when it sought to persuade social media platforms to review flagged posts.[172] During its switchboarding operations, CISA did not issue any threats, leaving the platforms free "to decide what action to take, if any."[173] Additionally, "CISA did not coordinate EIP's flagging of potentially violative material to the platforms, never gave EIP instructions about how the project should be conducted, and never pressured or directed EIP's conduct in any way."[174] The "EIP's decisions about what to escalate to social media platforms were made" independent of CISA.[175]

The opposing perspective, as outlined by the district court, is that CISA communicated with social media platforms to pressure the platforms into suppressing Americans' speech.[176] Under this view, CISA satisfied *Blum's* "significant encouragement" standard[177] by

---

[169] *See* Lakier, *supra* note 137.
[170] *See* Clay Calvert, *Persuasion or Coercion? Understanding the Government's Position in Murthy v. Missouri, Part II*, AM. ENTER. INST. (Jan. 10, 2024), https://www.aei.org/technology-and-innovation/persuasion-or-coercion-understanding-the-governments-position-in-murthy-v-missouri-part-ii/.
[171] *See* Nat'l Rifle Ass'n of Am. v. Vullo, 602 U.S. 175, 190 (2024) (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963)).
[172] *See* Brief for the Petitioners at 39, Murthy v. Missouri, 603 U.S. 43 (2024) (No. 23-411).
[173] *Id.* at 30.
[174] Brief for Stanford University, *supra* note 110, at 24.
[175] *See id.* at 25.
[176] *See* Missouri v. Biden, 680 F. Supp. 3d 630, 703 (W.D. La.), *aff'd in part*, *rev'd in part*, *vacated in part*, 83 F.4th 350 (5th Cir. 2023), *rev'd sub nom.* Murthy v. Missouri, 603 U.S. 43 (2024).
[177] *See* Brief of Respondents at 31-33, Murthy v. Missouri, 603 U.S. 43 (2024) (No. 23-411) (quoting Blum v. Yaretsky, 457 U.S. 991, 1004 (1982)).

repeatedly switchboarding information to social media platforms, even during evenings and weekends.[178] The Fifth Circuit found that the platforms relied on "CISA's determination[s] of the veracity of . . . flagged information" when making censorship decisions.[179] Moreover, the district court also noted that CISA worked in conjunction with CIS and the EIP, two private actors, to identify and report Americans' speech to social media platforms.[180]

In 2024, this issue reached the Supreme Court in *Murthy v. Missouri*.[181] Two years prior, the attorneys general of Missouri and Louisiana filed a lawsuit against federal officials, including the director of CISA, for unconstitutionally censoring Americans' speech.[182] The Supreme Court reversed the Fifth Circuit and held that Missouri and Louisiana, and five platform users, lacked standing.[183] Because the Court did not discuss the merits of the case,[184] determining whether the government unconstitutionally jawboned social media platforms into suppressing Americans' speech remains tricky.[185]

III. NEXT STEPS

In light of this "[d]octrinal [d]isarray,"[186] and the Court's decision in *Murthy v. Missouri*,[187] a shift in focus from the Court to Congress is needed to address government jawboning on social media platforms.[188] But what should Congress do? Among the possibilities

---

[178] *See id.* at 33 (noting that the record included evidence that CISA officials switchboarded content after hours).
[179] *See* Missouri v. Biden, 83 F.4th 350, 391 (5th Cir. 2023), *rev'd sub nom.* Murthy v. Missouri, 603 U.S. 43 (2024).
[180] *See* Missouri v. Biden, 680 F. Supp. 3d at 704.
[181] *See generally* Murthy v. Missouri, 603 U.S. 43 (2024).
[182] *See generally* Complaint, Missouri v. Biden, 680 F. Supp. 630 (W.D. La. 2023) (No. 3:22-cv-01213).
[183] *See* Murthy v. Missouri, 603 U.S. at 49, 76.
[184] *Id.* at 55 n.3.
[185] *See* Lakier, *supra* note 137.
[186] *See* Teitler, *supra* note 136.
[187] *See* Murthy v. Missouri, 603 U.S. at 55 n.3.
[188] *See* Andrew M. Grossman & Kristin A. Shapiro, *Shining a Light on Censorship: How Transparency Can Curtail Government Social Media Censorship and More*, CATO INST.: BRIEFING PAPER NO. 168, at 4 (Oct. 3, 2023) https://www.cato.org/sites/cato.org/files/2023-09/BP%20168_update.pdf ("These

for legislative action, Congress should seek to foster government transparency[189] and leverage technology-based expediency.[190] Further, Congress can balance these tenets with security to mitigate potential risks, including legitimate national security concerns, arising from a "transparency-based approach."[191]

One term has consistently dominated legislative-centered discussions about this issue—transparency.[192] As scholars have argued, the first step Congress should take to address government jawboning of speech is to require greater transparency.[193] Thus, if the government refers speech to a social media platform that it believes is harmful, "it should make that referral public, and not just transmit it . . . in secret."[194] During the 2020 election season, CISA's efforts were engulfed in secrecy.[195] Even now, only a fraction of these efforts have been made public.[196] This approach "would reveal the hand of government, where it exists, from the get-go."[197] Transparency would, in theory, give the public the facts necessary to understand the government's conduct—especially when that conduct affects

precedents demonstrate that it will be difficult for First Amendment litigation to operate as a comprehensive check on censorship by proxy.").

[189] *See infra* text accompanying notes 192-99.

[190] *See infra* text accompanying notes 200-08.

[191] *See* Grossman & Shapiro, *supra* note 188, at 6.

[192] *See, e.g.*, Mark MacCarthy, *Government Efforts to Censor Social Media Should be Transparent*, FORBES (Oct. 5, 2022, 4:18 PM), https://www.forbes.com/sites/washingtonbytes/2022/10/05/government-efforts-to-censor-social-media-should-be-transparent/.

[193] *See, e.g.*, *Censorship Laundering*, *supra* note 80, at 53 (prepared statement of Jonathan Turley, Shapiro Professor of Public Interest Law, George Washington University Law School); *see also id.*

[194] MacCarthy, *supra* note 192.

[195] *See Censorship Laundering*, *supra* note 80, at 52 (prepared statement of Jonathan Turley, Shapiro Professor of Public Interest Law, George Washington University Law School).

[196] *See id.* at 42.

[197] Grossman & Shapiro, *supra* note 188, at 6.

speech.[198] And these facts, when made public, would be critical in facilitating future litigation efforts.[199]

If Congress pursued a "transparency-based approach,"[200] the government should consider the role artificial intelligence ("AI"), and other emerging technologies, could have in this reporting process[201] to ensure these communications are published expeditiously.[202] With some variation, scholars and lawmakers have proposed legislation that would require government officials to report suppression attempts to the Director of the Office of Management and Budget ("OMB"), who would then review and publish the information within a fixed timeframe.[203] Human-led, pre-publication review is possible,[204] but

---

[198] *See Censorship Laundering*, *supra* note 80, at 54 (prepared statement of Jonathan Turley, Shapiro Professor of Public Interest Law, George Washington University Law School).

[199] Grossman & Shapiro, *supra* note 188, at 6.

[200] *See id.* at 2 (arguing in support of a "transparency-based approach" to counteract jawboning).

[201] *Compare* Howard Langsam, *Want to Beat FOIA Backlogs? Embrace AI*, AITHORITY (June 26, 2024), https://aithority.com/machine-learning/want-to-beat-foia-backlogs-embrace-ai/ ("AI can also help government agencies in their quest to more proactively publish data and records to promote transparency . . . ."), *with* Lewis Kamb, *Some U.S. Government Agencies Are Testing Out AI to Help Fulfill Public Records Requests*, NBC NEWS (Aug. 1, 2023, 12:11 PM), https://www.nbcnews.com/news/us-news/federal-agencies-testing-ai-foia-concerns-rcna97313 ("[S]ome transparency advocates warn that the government needs additional safeguards before more widely deploying the technology.").

[202] *Cf. Processing FOIA Requests: How AI Helps LEAs and the Public*, VERITONE, https://www.veritone.com/blog/processing-foia-requests/ (last visited Mar. 30, 2025) ("The right AI technology can help human officers process data at a much faster rate . . . .").

[203] *See, e.g.*, Grossman & Shapiro, *supra* note 188, at 6; Will Duffield, *Toward a Jawboning Transparency Act*, KNIGHT FIRST AMEND. INST. AT COLUMBIA UNIV.: JAWBONING (Oct. 19, 2023), https://knightcolumbia.org/blog/toward-a-jawboning-transparency-act; *Social Media Administrative Reporting Transparency (SMART) Act DRAFT*, FOUND. FOR INDIVIDUAL RTS. AND EXPRESSION (May 20, 2024), https://www.thefire.org/research-learn/social-media-administrative-reporting-transparency-smart-act-draft-may-20-2024; Disclose Government Censorship Act, S. 2527, 117th Cong. § 3 (2021); Accountability for Government Censorship Act, H.R. 1162, 118th Cong. § 2 (2023); Free Speech Protection Act, S. 2425, 118th Cong. § 5 (2023).

[204] *See, e.g.*, *Information Management Division (IMD) Pre-Publication Review – Frequently Asked Questions*, OFF. OF THE DIR. OF NAT'L INTEL.,

information-release procedures, such as Freedom of Information Act ("FOIA") requests, are often plagued by bureaucratic delays.[205] While debates over the implementation of AI in government are ongoing,[206] and beyond the scope of this Comment, "responsible AI *can* modernize federal programs."[207] Thus, leveraging AI to expedite a "transparency-based approach"[208] could improve the reporting process and reduce similar opportunities for delay.

While different viewpoints regarding transparency exist,[209] one blanket concern is "that transparency would endanger national security."[210] But a "transparency-based approach," that includes an element of technology-based expediency, can be safely achieved when balanced with privacy and security interests.[211] While Congress is better suited to determine this balance, these two interests are especially relevant in cases involving government jawboning of speech on social media—and both interests can be safeguarded under this approach.[212] First, as scholars have proposed, a "transparency-based

https://www.dni.gov/files/documents/Pre%20Pub%20FAQs.pdf (last visited Mar. 31, 2025).

[205] *See FOIA Backlogs Hinder Government Transparency and Accountability*, U.S. GOV'T ACCOUNTABILITY OFF.: WATCHBLOG (Mar. 14, 2024), https://www.gao.gov/blog/foia-backlogs-hinder-government-transparency-and-accountability; *see also Federal Information Transparency*, U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/federal-information-transparency (last visited Mar. 30, 2025).

[206] *See, e.g.*, David Freeman Engstrom et al., *AI's Promise and Peril for the U.S. Government*, STAN. UNIV. HUMAN-CENTERED A.I. 5 (Sept. 2020), https://hai.stanford.edu/sites/default/files/2020-09/HAI_PromisePeril_Sep20.pdf.

[207] *See* Daniel E. Ho, *Opportunities and Risks of Artificial Intelligence in the Public Sector*, STAN. L. SCH. BLOGS: LEGAL AGGREGATE (May 25, 2023) (emphasis added), https://law.stanford.edu/2023/05/25/opportunities-and-risks-of-artificial-intelligence-in-the-public-sector/#slsnav-i-the-importance-of-public-sector-ai.

[208] *See* Grossman & Shapiro, *supra* note 188, at 2.

[209] *See, e.g.*, Matthew Yglesias, *Against Transparency*, VOX (Sept. 6, 2016, 8:30 AM), https://www.vox.com/2016/9/6/12732252/against-transparency ("We need to let public officials talk to each other — and to their professional contacts outside the government — in ways that are both honest and technologically modern.").

[210] *See* Kade Crockford, *How State Secrecy Protects Government Agencies from Embarrassment, Then and Now*, ACLU TEX. (Mar. 31, 2014, 8:12 AM), https://www.aclutx.org/en/news/how-state-secrecy-protects-government-agencies-embarrassment-then-and-now.

[211] *See* Grossman & Shapiro, *supra* note 188, at 6.

[212] *See id.*

approach" should contain a redaction mechanism to protect a user's privacy and other identifying information.[213] Second, if an official forwards a user's post to a social media platform due to national security concerns, that communication should not be subject to expedient release.[214] In the end, a balanced approach should be used to highlight government jawboning, not unprotected speech.[215]

CONCLUSION

The Framers designed the First Amendment as a form of protection against government-sponsored censorship.[216] Today, however, "jawboning as a species of First Amendment violation is alive and well."[217] Examining CISA's recent attempts to combat MDM[218] presents a helpful case study on the application of jawboning in the digital age. But determining whether CISA, or other government agencies, unconstitutionally coerced social media platforms into suppressing disfavored speech[219] remains unresolved.[220] While there have been executive steps to curb the specific actions discussed in this case study,[221] jawboning is always possible, especially in the digital age. For now, the responsibility lies with Congress to craft a legislative

---

[213] *Id.* at 6-7.
[214] *See id.*
[215] *See id.*
[216] *See Censorship Laundering*, *supra* note 80, at 49 (prepared statement of Jonathan Turley, Shapiro Professor of Public Interest Law, George Washington University Law School).
[217] Derek E. Bambauer, *The Jawboning Cases End with a Bang Disguised by a Whimper*, 2023-2024 CATO SUP. CT. REV. 157, 158, https://www.cato.org/sites/cato.org/files/2024-09/cato-supreme-court-review-2023-2024-7.pdf.
[218] *See* UNIVERSITY REPORT, *supra* note 81, at 8.
[219] *See* Nat'l Rifle Ass'n of Am. v. Vullo, 602 U.S. 175, 190 (2024) (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963)).
[220] *See* Greene, *supra* note 135.
[221] *See, e.g.*, Exec. Order No. 14149, 90 Fed. Reg. 8243 (Jan. 20, 2025); s*ee also* Derek B. Johnson, *CISA Election, Disinformation Officials Placed on Administrative Leave, Sources Say*, CYBERSCOOP (Feb. 10, 2025), https://cyberscoop.com/cisa-misinformation-disinformation-administrative-leave/.

solution that shines a light on this conduct[222] in an expedient and secure manner.

[222] *See* Grossman & Shapiro, *supra* note 188, at 1.