Fordham Law Voting Rights and Democracy Forum

Volume 2 | Issue 2

March 2024

Spies, Trolls, and Bots: Combating Foreign Election Interference in the Marketplace of Ideas

Nahal Kazemi
Chapman University Fowler School of Law

SPIES, TROLLS, AND BOTS: COMBATING FOREIGN ELECTION INTERFERENCE IN THE MARKETPLACE OF IDEAS

Nahal Kazemi[*]

Foreign disinformation operations on social media pose a significant and rapidly evolving risk, particularly when aimed at American elections. We must urgently and effectively address this form of election interference. This Article examines potential responses to those risks, through a review of the unique characteristics, both practical and legal, of political advertising on social media platforms. This Article analyzes proposed legislative responses to foreign disinformation, noting that no single proposed law to date adequately addresses the threats and challenges posed by foreign disinformation.

This Article considers the election law landscape in which the proposed laws would operate. It evaluates the proposed legislative responses for judicial review resilience, with a focus on the First Amendment challenges to regulating political advertisement microtargeting—the use of data mining and algorithms to microtarget particular audiences. Some scholars have argued that a fundamental change in how we understand and therefore regulate social media in society is necessary to prevent the abuse of the First Amendment. This Article, however, approaches the problem from the position that the U.S. Supreme Court is highly unlikely to abandon its extremely robust interpretation of the First Amendment to impose broad restrictions on online platforms. The Article argues that an appropriate response to the threat of disinformation must be consistent with robust protections for political speech and with the First Amendment theory of a "marketplace of ideas."

This Article then reviews the role that various actors—from state and federal agencies to social media platforms, and academics and researchers—can play in crafting a "whole of society" response to disinformation operations.

INTRODUCTION 229

I. SOCIAL MEDIA PRESENTS UNIQUE VULNERABILITIES TO FOREIGN MISINFORMATION 237

A. Gaps in the Law 237

[*] Assistant Professor, Chapman University Fowler School of Law. The author wishes to thank Deepa Badrinarayana, Larry Rosenthal, Carrie Rosenbaum, Jason Schall, Adam Tullman, and Harrison Schweiloch for their invaluable feedback and assistance.

B. Social Media's Unique Features 238

1. Reach 238
2. Microtargeting Advertising Technology 239
3. Sharing and Virality 247

C. Artificial Intelligence 249

II. PROPOSED LEGISLATIVE RESPONSES 254

A. Examples of State-Level Attempts to Regulate Social Media Election Advertisements 255
B. Proposed Federal Legislative Responses 258

1. Honest Ads Act ("HAA") 258
2. Protecting Democracy from Disinformation Act ("PDDA") 261
3. REAL Political Advertisements Act ("RPAA") 263
4. Digital Consumer Protection Commission Act ("DCPCA") 264
5. Democracy is Strengthened by Casting Light on Spending in Elections Act of 2023 ("DISCLOSE Act") 265
6. Additional Legislative Responses to Consider 266

III. FIRST AMENDMENT IMPLICATIONS 267

A. First Amendment Jurisprudence: The Strongest Possible Protections for Political Speech 268
B. Possibilities for Regulating Microtargeting 272

1. Is Microtargeting Speech? 272
2. Arguments in Favor of the Constitutionality of Microtargeting Bans 274
3. Why Microtargeting Bans Will Likely Be Held Unconstitutional 275
4. Why Changing the First Amendment Paradigm for Disinformation Campaigns Will Fail 280

C. What About AI? 281
D. Foreign Actors Can Be Completely Excluded from Acts of Democratic Self-Governance 283

IV. WHOLE OF SOCIETY RESPONSES 284

CONCLUSION 292

INTRODUCTION

> *Against the insidious wiles of foreign influence (I conjure you to believe me, fellow-citizens) the jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republican government.*
>
> - George Washington, Farewell Address[1]

The efforts of foreign governments—and their closely-aligned non-state actors—to meddle in U.S. elections at the federal, state, and even local levels have been widespread and growing since at least 2016.[2] Russian influence operations were especially prevalent in the 2016 presidential election.[3] Leveraging the power of social media in new ways, the Russian government and its proxies purchased thousands of social media ads reaching at least ten million voters, primarily in swing states.[4] Not only does this disinformation risk confusing and misleading voters, but it is also often deployed for the specific purpose of undermining trust in government, institutions, and the press in a concerted effort to weaken democracy.

Social media advertising is an appealing venue for foreign influence operations for the same reasons that it appeals to good faith actors[5] seeking to reach their audiences. First, a huge

[1] George Washington, Farewell Address (1796). Transcript available at: https://constitutioncenter.org/the-constitution/historic-document-library/detail/george-washington-farewell-address-1796 [perma.cc/M7RX-9WNS].

[2] *See generally* Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, COMPUTATIONAL PROPAGANDA RSCH. PROJECT (2018) (analyzing Russia's Internet Research Agency's use of computational propaganda to misinform and polarize U.S. voters), https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf [perma.cc/36GA-8X6V].

[3] *See* ROBERT S. MUELLER, III, U.S. DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION, VOL. I OF II, at 23 (2019) [hereinafter MUELLER REPORT, VOL. 1].

[4] *See* Trevor Potter, *Foreign Interference in the 2016 Election: How Did We Get Here?*, CAMPAIGN L. CTR. 1, 3 (2018).

[5] The phrase "good faith actors" is used here to describe domestic political actors—such as campaigns, parties, and third-party interest groups—that seek to disseminate messages that are not knowingly false, misleading, or deceptive. No normative judgment is intended in terms of the substance of those communications. In other words, it is possible for "good faith actors" to spread misinformation, i.e., to disseminate information that is wrong or misleading despite the actor's honest belief in the statement. Disinformation, on the other hand, is knowingly false, misleading, or deceptive information designed to confuse, anger, disorient, or demotivate an audience. As described herein,

percentage of the population is on social media and obtains news from it, as compared with traditional media.[6] Second, social media and search engine ads are inexpensive compared to traditional print, television, and radio media.[7] Third, microtargeting allows an advertiser to concentrate its message on the most receptive populations and to tailor communications to specific subpopulations.[8] Lastly, rich data analytics allow advertisers to better measure the efficacy of their advertisements by identifying who engages with the ads, for how long, and in which ways, such as liking or sharing a post, clicking through to the website, or engaging in a transaction. Advertisers can focus their efforts on the messages that work, constantly refining and recalibrating their message and targeting to optimize impact.[9]

The efficacy of foreign influence operations on American electoral politics remains debatable, but the risk is not.[10] Russia, China, North Korea, Iran, and other hostile powers will continue to engage in strategic disinformation campaigns against our elections as well as those of our allies and other democratic states.[11] The rise

disinformation does not necessarily seek to convince an audience that what is being said is true. Rather, it is often used to undermine faith in public discourse and the political process writ large. *See* YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 32, 36 (2018).

[6] *See* Honest Ads Act, S. 1356, 116th Cong. § 3(5), 3(7) (2019) ("The reach of a few large internet platforms—larger than any broadcast, satellite, or cable provider—has greatly facilitated the scope and effectiveness of disinformation campaigns. For instance, the largest platform has over 210,000,000 American users—over 160,000,000 of them on a daily basis. By contrast, the largest cable television provider has 22,430,000 subscribers, while the largest satellite television provider has 21,000,000 subscribers. And the most-watched television broadcast in U.S. history had 118,000,000 viewers.").

[7] *See generally* Lata Nott, *Political Advertising on Social Media Platforms*, A.B.A. HUM. R. MAG., VOL. 45, NO. 3: VOTING IN 2020 (June 25, 2020), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/voting-in-2020/political-advertising-on-social-media-platforms [perma.cc/K78G-MDVH]; BENKLER ET AL., *supra* note 5, at 329.

[8] *See generally* Nott*, supra* note 7.

[9] *See* Julie E. Cohen, *Tailoring Election Regulation: The Platform Is the Frame*, 4 GEO. L. TECH. J., 641, 647-48 (2020); Aashish Pahwa, *What Is Microtargeting?*, FEEDOUGH (Aug. 4, 2023), https://www.feedough.com/what-is-microtargeting [perma.cc/7B2V-HWL2].

[10] *See* BENKLER ET AL., *supra* note 5, at 254–68.

[11] *See generally* Press Release, U.S. Dep't of Just., U.S. Citizens and Russian Intelligence Officers Charged with Conspiring to Use U.S. Citizens as Illegal Agents of the Russian Government (Apr. 18, 2023), https://www.justice.gov/opa/pr/us-citizens-and-russian-intelligence-officers-charged-conspiring-use-us-citizens-illegal) [perma.cc/N2UU-KDTC]; Sam Sabin, *Iran Is Diving into the Disinformation Wars, Microsoft Says*, AXIOS (May 2, 2023), https://www.axios.com/2023/05/02/iran-disinformation-wars-microsoft [perma.cc/64MX-HURU]; SCOTT W. HAROLD ET AL., CHINESE DISINFORMATION EFFORTS ON SOCIAL MEDIA (2021) (ebook),

of written media, audio, and video produced by artificial intelligence will only exacerbate this trend as it will bring the cost of generating believable disinformation to essentially zero.[12]

Given the open nature of the internet in the United States, the ease with which bad actors can hide their intentions and identities, and the robustness of American protections for free speech, limiting the impact of foreign disinformation through social media is an extremely difficult challenge. But while it would be impossible to completely eliminate foreign disinformation targeting the American political process, certain steps toward safeguarding our democratic processes from foreign interference are possible.

In recent years, several legislative proposals, both at the state level and in Congress, have attempted to address this problem. But as this Article describes, none of these attempts fully encompasses the appropriate steps necessary to counter foreign disinformation operations in ways consistent with the First Amendment. A disclosure-based approach, drawing from many of the proposed legislative solutions, can both limit foreign disinformation efforts and strengthen the "marketplace of ideas"[13] for political speech.

To properly address the threat of disinformation, we must first consider what interests we are attempting to protect. Simply

https://www.rand.org/pubs/research_reports/RR4373z3.html [perma.cc/HX4U-9EEX]; Seong H. Choi, *North Korea's Provocative and Secret Interventions in South Korean Election*s, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 7, 2022), https://www.csis.org/blogs/new-perspectives-asia/north-koreas-provocative-and-secret-interventions-south-korean [perma.cc/XHB5-Z7WT].

[12] Tiffany Hsu & Stuart A. Thompson, *Disinformation Researchers Raise Alarms About A.I. Chatbots*, N.Y. TIMES (Feb. 8, 2023), https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation [perma.cc/93S9-DWBR]; *see also* Kevin T. Frazier, *Sounding the Alarm: AI's Impact on Democracy and News Integrity*, FORDHAM L. VOTING RTS. & DEMOCRACY F. COMMENT. (Jan. 25, 2024, 1:30 PM), https://fordhamdemocracyproject.com/2024/01/22/government-should-act-to-address-how-ai-is-polluting-our-information-ecosystem [perma.cc/8ZC5-XE32].

[13] The idea that false speech does not need to be suppressed, because, in a free society, it will encounter truth, and truth will ultimately prevail, has a long history in the Anglo-American legal and philosophical tradition. It dates back as far as John Milton's *Areopagitica,* an argument to the English Parliament against the requirement that all publishing be licensed and subject to censorship, published in 1644. *See generally* JOHN MILTON, AREOPAGITICA A SPEECH FOR THE LIBERTY OF UNLICENSED PRINTING TO THE PARLIAMENT OF ENGLAND (Auckland: The Floating Press 2009) (1644). The concept of a "marketplace of ideas" is often credited to John Stuart Mill. *See* JOHN STUART MILL, ON LIBERTY (Andrews U.K. Ltd. 2011) (1859). President Thomas Jefferson echoed similar ideas, arguing in his first inaugural address that it was safe to tolerate "error of opinion . . . Where reason is left free to combat it." President Thomas Jefferson, First Inaugural Address (Mar. 4, 1801), https://avalon.law.yale.edu/19th_century/jefinau1.asp [perma.cc/49RC-YEFA]. The concept made its way into American constitutional jurisprudence in Justice Oliver Wendell Holmes's famous dissent in *Abrams v. United States,* 250 U.S. 616, 630 (1919).

stated, a functioning democracy depends on an informed electorate.[14] For the electorate to be informed, it must be able to weigh the trustworthiness of the information presented. Particularly when the information originates from abroad, we have an interest in understanding why the speaker is trying to influence an election in a country other than their own. When it comes to foreign efforts to influence American elections through social media advertising, both the government and the public have a compelling interest in knowing (1) who is speaking; (2) what they are saying; and (3) to whom. Without this key information, end users cannot properly evaluate the messages they are receiving, undermining a core tenet of our First Amendment jurisprudence: more information is the solution to bad information.[15]

The last factor—to whom the advertiser is speaking—is a relatively new concern. This is because older advertising methods, like network television ads or mailed campaign literature, either cannot be as finely targeted, or the targeting is obvious, like when a speaker delivers a speech at a club meeting or church. On social media, however, advertising is often highly targeted to the user—ads may be based on prior engagement, what profile information the user voluntarily shared, or cookies related to factors such as internet shopping and browsing habits. But, unlike in more traditional

[14] Democracy scholars are largely in agreement that a democratic society depends on an informed electorate to function properly. *See, e.g.,* MICHAEL X. DELLI CARPINI & SCOTT KEETER, WHAT AMERICANS KNOW ABOUT POLITICS AND WHY IT MATTERS 5 (1996) ("…knowledge is a keystone to other civic requisites. In the absence of adequate information neither passion nor reason is likely to lead to decisions that reflect the real interests of the public."); *see also,* Kevin T. Frazier, *Sounding the Alarm: AI's Impact on Democracy and News Integrity*, FORDHAM L. VOTING RTS. & DEMOCRACY F. COMMENT. (Jan. 25, 2024, 1:30 PM), https://fordhamdemocracyproject.com/2024/01/22/government-should-act-to-address-how-ai-is-polluting-our-information-ecosystem [perma.cc/MWY5-8AJQ]. *But see,* Jennifer L. Hochschild, *If Democracies Need Informed Voters, How Can They Thrive While Expanding Enfranchisement?*, 9 ELECTION L.J. 111, 111 (2010) (noting the broad consensus among political theorists about the importance of informed citizenry to functioning democracy and exploring the paradox of how expanding the franchise to marginalized groups, which have tended to have lower educational levels, has nonetheless resulted in a government we view as more democratic).

This modern consensus hearkens back to the very founding of the United States, as evidenced, for example, by Thomas Jefferson's letters. *See* Letter from Thomas Jefferson to Richard Price (Jan. 8, 1789) (on file at the Library of Congress), https://www.loc.gov/exhibits/jefferson/60.html ("[W]herever the people are well informed they can be trusted with their own government[.]") [perma.cc/VF52-NJH6]; Letter from Thomas Jefferson to Charles Yancey (Jan. 6, 1816) (on file at the Library of Congress), https://www.loc.gov/resource/mtj1.048_0731_0734/?sp=4&st=text [perma.cc/NKM7-6SFP] ("If a nation expects to be ignorant and free, in a state of civilisation, it expects what never was and never will be.").

[15] *See Abrams*, 250 U.S. at 630 (Holmes, J., dissenting).

campaigning fora, a user may not as easily discern what information went into the advertisers' decision to target them.[16] Election laws regulating advertising in other media include disclosure laws and "stand by your ad," requirements, which address the issue of who is speaking and what they are saying.[17] Existing regulation of newer types of voter communication targeting has not focused on *how* an audience is targeted.[18]

More generally speaking, election campaign laws have not kept up with social media and search engine advertising, creating a vast, practically unregulated space in which bad actors—foreign and domestic—can spread and amplify disinformation, propaganda, and conspiracy theories, all while obscuring their own identities, methods, and reasons for targeting particular audiences.[19] In some instances, these efforts may be directed at helping favored candidates win office. But when it comes to foreign influence operations, there is evidence of a broader and even more invidious strategic aim: not just to sway the outcome of a particular election, but to undermine the legitimacy of liberal democracy itself.[20] If

[16] Campaigns, political action committees ("PACs"), and interest groups often buy, sell, and share mailing lists, including through the use of social media. Often, a supporter signs up to be on one candidate or group's mailing list and then finds themselves getting emails from multiple candidates and campaigns, sometimes for the same office. *See* Karl Evers-Hillstrom & Camille Erickson, *Your Email Is for Sale — And 2020 Candidates Are Paying Up*, OPENSECRETS (June 13, 2019, 11:17 AM) https://www.opensecrets.org/news/2019/06/email-list-for-sale-2020-candidates-are-paying/. To date, this form of audience selection has not used the same sort of microtargeting that online social media ads use, though there are efforts to focus on the email addresses of those most likely to donate. *Id.*

[17] *See* Bipartisan Campaign Reform Act of 2002, H.R. 2356, 107th Cong. (2002) (enacted as Public Law 107–155, 116 Stat. 81). For state-by-state political ad disclosure laws, see *Disclaimers on Political Advertisements*, NAT'L CONF. OF STATE LEGISLATURES (Mar. 14, 2023), https://www.ncsl.org/elections-and-campaigns/disclaimers-on-political-advertisements [perma.cc/W4TE-DZD7].

[18] See, for example, California's Social Media DISCLOSE Act, A.B. 2188, State Assemb., 2017-2018 Sess., § 2 (Cal. 2018) (codified in scattered sections of CAL. GOV. CODE §§ 84501-84510 (2023)), which requires online ads to identify who paid for them, but does not require disclosure of the use of algorithms or microtargeting to target particular audiences.

[19] *See* Honest Ads Act, S. 1356, 116th Cong. § 3(10) (2019) ("In testimony before the Senate Select Committee on Intelligence titled, 'Disinformation: A Primer in Russian Active Measures and Influence Campaigns,' multiple expert witnesses testified that while the disinformation tactics of foreign adversaries have not necessarily changed, social media services now provide 'platform[s] practically purpose-built for active measures[.]'"); *id.* at § 3(11) ("Current regulations on political advertisements do not provide sufficient transparency to uphold the public's right to be fully informed about political advertisements made online.").

[20] *See* Indictment at 4, United States v. Internet Research Agency LLC, No. 1:18-cr-32 (D.D.C. Feb. 16, 2018), https://www.justice.gov/file/1035477; S. COMM. ON INTEL., 116TH CONG., REP. OF THE SELECT COMMITTEE ON INTELLIGENCE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 ELECTION, VOL. 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE

elections cannot be trusted, if they are vulnerable to manipulation, and if the public has no faith in either the process or the substantive information public officials communicate, the connective tissue holding together representative self-governance could be destroyed.[21]

State and federal legislators have put forward several proposals to fill the gaps in election law regarding disinformation. Some of these proposals seek to enhance disclosure requirements.[22] Others are targeted at excluding foreign actors.[23] Still others seek to prohibit or limit the use of technology to direct ads to particular audiences.[24] This last category of regulation—limiting the ability to target online audiences with political ads—will raise First Amendment concerns: Is it constitutionally permissible to regulate or prohibit the use of algorithms and other digital tools designed to target an audience? If so, under what circumstances?

Others have argued that a fundamental change in how we understand and therefore regulate social media is necessary to prevent the abuse of the First Amendment.[25] This Article, however, approaches the problem from the position that the U.S. Supreme Court is highly unlikely to abandon its extremely robust interpretation of the First Amendment to impose broad restrictions on online platforms. As such, this Article argues that it is possible to craft appropriate responses to disinformation threats that are consistent with the robust protections for political speech in First Amendment jurisprudence. To date, no proposed legislation achieves an ideal balance.

It is important to note that foreign influence operations are not the only type of disinformation in the American electoral landscape. Plenty of domestic actors, from political candidates to media outlets and interest groups, have made false statements,[26]

WITH ADDITIONAL VIEWS 5 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [perma.cc/L9DD-NQ85]; *see generally* Christina Nemr & William Gangaware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, PARK ADVISORS (Mar. 2019), https://www.state.gov/weapons-of-mass-distraction-foreign-state-sponsored-disinformation-in-the-digital-age [perma.cc/EDJ4-25XW].

[21] *See generally* BENKLER ET AL., *supra* note 5.

[22] *See, e.g.*, CAL. GOV. CODE §§ § 84504.3-84504.4, 84504.6 (West 2023) (California's laws relating to disclosure on social media disclosure, requiring that online ads identify who paid for them).

[23] S*ee* N.Y. ELEC. LAW §§ 14-106, 14-107 (McKinney, Westlaw through L.2019, ch. 758 and L.2020, chs. 1 to 347) (prohibiting campaign spending by foreign entities).

[24] *See, e.g.*, Banning Microtargeted Political Ads Act, H.R. 7014, 117th Cong. (2021).

[25] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016).

[26] BENKLER ET AL., *supra* note 5, at 83–85.

thereby also perpetuating election disinformation. Propagation of the Big Lie—the false assertion that the 2020 election was stolen from former President Donald Trump—has only worsened this dynamic.[27]

Under First Amendment jurisprudence, the American legal system takes a relatively hands-off approach to domestic disinformation. The law generally does not regulate the substance of political speech. There are a few exceptions, like protections against interference with the right to vote[28] and electioneering close in time and place to an election,[29] as well as the limited categories of speech that are wholly unprotected, like defamation[30] and true threats.[31] But political candidates and campaigns are legally free to make blatantly false statements. The response our government considers appropriate is not sanctioning their speech, but for it to be challenged in the robust marketplace of ideas.[32]

Domestic disinformation is often aimed at achieving a particular political outcome—a win for one side over the other.[33] On the other hand, foreign disinformation typically has a different goal. It often seeks to undermine democracy itself by convincing the electorate that "everything [is] possible and that nothing [is] true."[34] By attacking the very idea that there are knowable, verifiable facts that should form the basis of political dialogue, these foreign actors seek to undermine the mechanisms of democratic self-governance.[35]

[27] *See* Gabriel R. Sanchez & Keesha Middlemass, *Misinformation is Eroding the Public's Confidence in Democracy*, BROOKINGS (July 26, 2022), https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy [perma.cc/X7ZP-VFKT].

[28] *See, e.g.,* 18 U.S.C. § 241; Press Release, U.S. Att'y's Office, E.D.N.Y., Social Media Influencer Douglass Mackey Sentenced After Conviction For Election Interference in 2016 Presidential Race (Oct. 18, 2023), https://www.justice.gov/usao-edny/pr/social-media-influencer-douglass-mackey-convicted-election-interference-2016 [perma.cc/8FVS-4C69]. Voter intimidation is also proscribed as a type of interference with the right to vote. *See* 18 U.S.C. § 594.

[29] *See* Burson v. Freeman*,* 504 U.S. 191, 193, 195, 211 (1992).

[30] *See* New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964).

[31] *See* Virginia v. Black, 538 U.S. 343, 359 (2003).

[32] *See, e.g.*, Red Lion Broad. Co. v. Fed. Commc'n Comm'n, 395 U.S. 367, 390 (1969).

[33] As described *infra* Section III.D, the government's tools for countering foreign disinformation are broader than those available to counter domestic disinformation, because regulation of foreign actors does not implicate the same concerns about infringing on citizens' acts of democratic self-governance. The effort to combat domestic disinformation is thus more challenging and complex. It is also beyond the scope of this Article.

[34] *See* HANNAH ARENDT, ORIGINS OF TOTALITARIANISM 382 (Meridian Books 1968).

[35] *See generally* NATIONAL INTELLIGENCE COUNCIL, FOREIGN THREATS TO THE 2020 U.S. FEDERAL ELECTIONS 3–4, 6 (2021).

United States law gives Congress and state governments significant leeway to exclude foreign actors from acts of political self-governance, allowing them to essentially outlaw foreign-funded election advertising.[36] But even where such rules exist, foreign disinformationists go to great efforts to evade them, often by disguising themselves as domestic actors. Pretending to be Americans not only provides the cover necessary to attempt to influence opinions but also gives entrée into the spaces where democratic dialogue takes place, including social media. Through social media advertising, foreign disinformationists amplify and repeat, through automated "bot" and paid "sockpuppet" accounts, their own and others' content advancing their agenda.[37]

Foreign bad actors intentionally interact with domestic actors, benign and potentially malign. They pretend to be American. They copy, amplify, and engage with content from actual domestic actors.[38] As a result, distinguishing purely foreign disinformation from domestic disinformation content is difficult, if not impossible. So even though, in theory, foreign actors can be completely excluded from political advertising without implicating the First Amendment,[39] efforts to address the risks from foreign disinformation will impact communications from domestic sources as well, potentially implicating free speech concerns. Indeed, the legislative efforts described in this Article do not attempt to address foreign disinformation in a vacuum—these proposed legislative responses would affect both domestic and foreign political speech, albeit not in exactly the same manner.

Part I of this Article will first consider social media's unique vulnerabilities to foreign political influence operations and the regulatory gaps exploited by bad actors, foreign and domestic, in this space. Part II analyzes proposed legislation to address these gaps, including the bipartisan Honest Ads Act ("HAA"), the Protecting Democracy from Disinformation Act ("PDDA"),[40] the DISCLOSE Act, the REAL Political Ads Act ("RPAA"), and, finally, the bipartisan Digital Consumer Protection Commission Act of 2023 ("DCPCA"). Part III then considers arguments as to whether these proposed regulatory measures are likely to withstand judicial scrutiny, and suggests a more narrowly tailored means of

[36] *See, e.g.*, Bluman v. Fed. Election Comm'n*,* 800 F. Supp. 2d 281, 283 (2011), *aff'd*, 565 U.S. 1104 (2012).

[37] *See* BENKLER ET AL., *supra* note 5, at 240–41.

[38] *Id.*

[39] *See, e.g.*, *Bluman*, 800 F. Supp. 2d at 283–84 (upholding a congressional ban on non-citizens and non-permanent residents making political contributions).

[40] Representative Cicilline retired from Congress in May 2023. It is not clear if any other members of Congress will sponsor future versions of the PDDA, but it is analyzed here as an important example of efforts to regulate microtargeting in political advertisements, an issue that is not likely to recede in importance.

regulating social media microtargeting. This narrower approach—anchored in disclosure and consent, rather than prohibition—is better positioned to survive the strict scrutiny courts apply to regulations that affect political speech,[41] and is consistent with the legal theory that robust political speech enables a freewheeling marketplace of ideas. Finally, Part IV considers the extent to which we may need to adjust traditional efforts to expose and deter disinformation, including a "whole of society" approach involving coordinated interagency efforts, transnational cooperation, and different levels of government, as well as private sector actors.

I. SOCIAL MEDIA PRESENTS UNIQUE VULNERABILITIES TO FOREIGN MISINFORMATION

A. Gaps in the Law

Barack Obama's 2008 presidential campaign was one of the first to effectively use social media advertising, with 10 percent of total ad spending directed to online sources.[42] In the 2008 election cycle, political candidates spent a combined total of $22.25 million on online political ads.[43] By the 2016 cycle, that number was $1.4 billion—a sixty-three-fold increase in just eight years.[44] But, despite the explosion in popularity of digital and social media advertising, campaign communication laws have not kept up. For one, the Federal Election Commission ("FEC") has failed to apply disclosure requirements to online ads.[45] The agency's authorizing statute, the Federal Election Campaign Act, specifically identifies the types of media subject to regulation,[46] but predates the rise of social media and thus excludes ads on these platforms.

[41] Numerous Supreme Court decisions have cited disclosure requirements for political spending as requirements that will survive strict scrutiny. *See, e.g.*, Buckley v. Valeo, 424 U.S. 1, 74–76, 84 (1976); McConnell v. Fed. Election Comm'n, 540 U.S. 93, 137–141 (2003), *overruled by* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010); Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340, 369, 371 (2010); SpeechNow.org v. Fed. Election Comm'n, 599 F.3d 686, 696 (D.C. Cir. 2010).

[42] Irfon Watkins, *Take a Note from Obama's Campaign Playbook: Go Digital on Political Ad Spending*, FORBES (Sept. 23, 2015, 9:00 AM), https://www.forbes.com/sites/realspin/2015/09/23/take-a-note-from-obamas-campaign-playbook-go-digital-on-political-ad-spending/?sh=3713b4a979d2 [perma.cc/TY75-K3BM].

[43] *See* Nott, *supra* note 7.

[44] *Id.*

[45] Honest Ads Act, S. 1356, 116th Cong. § 3 (2019).

[46] *See* 52 U.S.C. § 30101(22) (current law defines "public communication" to mean "a communication by means of any broadcast, cable, or satellite communication, newspaper, magazine, outdoor advertising facility, mass mailing, or telephone bank to the general public, or any other form of general public political advertising.").

Consequently, the FEC cannot apply certain disclosure requirements to issue ads or electioneering ads, meaning ads distributed close in time to an election that do not explicitly endorse a candidate, but which feature positive or negative messages about candidates.[47] As a result of this lack of regulation, political ads on social media often do not identify who paid for them, or whether they are endorsed by a candidate, even though similar ads on television, radio, or in print would have such disclosures.[48]

When combined with super PAC or so-called "dark money" advertising,[49] a substantial percentage of the political ads audiences receive in many states[50] are not attributed to their sources. And while the U.S. Supreme Court has upheld a blanket exclusion of foreigners from activities of democratic self-governance,[51] the failure to apply disclosure laws and regulations to social media advertisements and the ability of super PACs and 501(c)(4) groups to shield their donors from disclosure provide ample opportunities for foreign actors to obscure their efforts to influence our elections. Finally, current election law allows foreign-controlled corporations (meaning entities with significant foreign ownership or management) to participate in campaigning and election advertising, with minimal restrictions.[52]

B. Social Media's Unique Features

1. Reach

[47] Honest Ads Act, S. 1356, 116th Cong. § 3 (2019).

[48] *Id.*

[49] Robert Maguire, *$1.4 Billion and Counting in Spending by Super PACS, Dark Money Groups*, OPENSECRETS (Nov. 9, 2016, 4:47 PM), https://www.opensecrets.org/news/2016/11/1-4-billion-and-counting-in-spending-by-super-pacs-dark-money-groups/.

[50] Some states have adopted more stringent disclosure laws for traditional and social media advertising. In California, for example, under AB 2188, the Social Media DISCLOSE Act, online advertisements must include their sources or a link in the ad labeled "Who paid for this ad?" that goes to a website disclosing its major sources of financial support. *See* 2018 Cal. Legis. Serv. Ch. 754.

[51] Bluman v. Fed. Election Comm'n, 800 F. Supp. 2d 281 (2011), *aff'd*, 565 U.S. 1104 (2012) (holding that a law prohibiting foreign nationals—meaning foreign citizens except those who have been admitted as lawful permanent residents of the United States—from making political campaign contributions withstands strict scrutiny).

[52] Michael Sozan, *Fact Sheet: Stopping Political Spending by Foreign-Influenced U.S. Corporations*, CTR. FOR AM. PROGRESS (May 3, 2022), https://www.americanprogress.org/article/fact-sheet-stopping-political-spending-by-foreign-influenced-u-s-corporations/.

Social media's role as a source of news and information has grown dramatically over the past two decades. In 2005, 5 percent of American adults were regular users of social media.[53] Today, 68 percent of Americans are on Facebook and 83 percent use YouTube.[54] According to Pew Research, 18 percent of all Americans used the Internet as their primary source of news about the 2004 presidential election.[55] Just ten years later, Pew determined that 65 percent of Americans identified an internet-based source as their leading source of information for the 2016 election.[56] In the 2020 election cycle, Meta and Google—purveyors of some of the most popular platforms, such as Facebook, Instagram, and YouTube, and the two largest sellers of online advertising—collected hundreds of millions of dollars in campaign spending from presidential candidates Donald Trump and Joe Biden,[57] in addition to hundreds of millions more from candidates for other offices, PACs, political parties, interest groups, and super PACs.[58]

2. Microtargeting Advertising Technology

As described above, social media advertising is more cost-effective and allows greater control and fine-tuning of messages to particular audiences than advertising in traditional forms of media. Campaigns achieve this fine-tuning by continuously testing different messages to determine which messages work best and then focusing their advertising dollars only on the efficacious messages. "A/B testing" is a method used by campaigns, behavioral marketing firms, and others to sample two different versions of the same message intended for a particular audience.[59] By comparing how the target demographic responds to alternative versions of the message, an advertiser can easily determine the more effective

[53] *Social Media Usage: 2005-2015*, PEW RSCH. CTR. (Oct. 8, 2015), https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/ [perma.cc/9SMG-GD4L].

[54] *Social Media Fact Sheet*, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/social-media [perma.cc/4FQJ-C5FN].

[55] *The Internet and Campaign 2004, Part II: The Role of the Internet in 2004*, PEW RSCH. CTR. (Mar. 6, 2005), https://www.pewresearch.org/internet/2005/03/06/part-2-the-role-of-the-internet-in-2004 [perma.cc/35KB-8XFY].

[56] Honest Ads Act, S. 1356, 116th Cong. § 3(8) (2019).

[57] Merrill Weber, *Reform for Online Political Advertising: Add On to the Honest Ads Act*, 74 FED. COMMC'N L.J. 81, 89 (2019).

[58] *Id.*; Sissi Cao & Jordan Zakarin, *Big Tech and CEOs Poured Millions into the Election. Here's Who They Supported*, OBSERVER (Nov. 2, 2020, 12:52 PM), https://observer.com/2020/11/big-tech-2020-presidential-election-donation-breakdown-ranking [perma.cc/W53Y-WMQK].

[59] BENKLER ET AL., *supra* note 5, at 271.

version, removing most of the guesswork from advertising.[60] During the 2016 election cycle, Facebook offered presidential campaigns the opportunity to embed Facebook staff into their campaign teams to assist with this and other microtargeting efforts.[61]

Additionally, because social media advertisements can be directed at small populations and can run for brief periods, they are far less likely to individually attract the attention of journalists, academics, or opposing political candidates who have a vested interest in exposing political misinformation or disinformation, or who may simply offer a competing viewpoint. In other words, if an advertiser can leverage social media platforms' extensive personal information about their users to target specific and relatively receptive demographics, they can delay scrutiny of that message from those more skeptical of it until it has already taken root and had a substantial impact.[62]

Foreign state and state-adjacent actors, including the Russian government-aligned Internet Research Agency,[63] specifically target susceptible audiences with outrageous, divisive, and conspiratorial content.[64] The strategic objectives of these disparate ads—ranging in topics from gun control and immigration to Black Lives Matter and crime—are to sow division and discord, reduce public trust, and erode confidence in electoral politics.[65] In 2016, fake Russian accounts (both automated "bot" accounts and ones controlled by actual human beings) pretending to be Americans, i.e., sockpuppets, disseminated divisive and inflammatory content as part of an active measures campaign[66] that was not fully exposed until after the election.[67]

In an op-ed in *The Washington Post*, FEC Chair Ellen L. Weintraub warned of the dangers of microtargeted political ads. She noted that "[i]t is easy to single out susceptible groups and direct political misinformation to them with little accountability because the public at large never sees the ad."[68] Chairwoman Weintraub

[60] *Id.*

[61] *Id.* at 272.

[62] *See* Cohen, *supra* note 9, at 649–52.

[63] While the Internet Research Agency is technically an independent company founded by notorious mercenary, Yevgeny Prigozhin, the organization has strong ties to the Russian government. U.S. SENATE SELECT COMM. ON INTEL., RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOLS. I-V, S. REP. NO. 116-290, at 5 (2019).

[64] MUELLER REPORT, VOL. 1, *supra* note 3, at 22.

[65] *See generally* William J. Aceves, *Virtual Hatred: How Russia Tried to Start a Race War in the United States*, 24 MICH. J.L. & RACE 177 (2019).

[66] H.R. REP. NO. 115-1110, at 10 (2018).

[67] *See generally id.*

[68] Ellen L. Weintraub, *Opinion, Don't Abolish Political Ads on Social Media. Stop Microtargeting*, WASH. POST (Nov. 1, 2019, 6:51 PM), https://www.washingtonpost.com/opinions/2019/11/01/dont-abolish-political-

described microtargeted political ads as "a potent weapon for spreading disinformation and sowing discord."[69] She advocated for eliminating microtargeting of political ads to "[e]nhance transparency and accountability" and "[d]eter and flush out disinformation."[70] There are currently no federal laws requiring platforms to publicly share how users are targeted with microtargeting tools.[71] This leaves platforms free to decide for themselves how to regulate political advertising microtargeting.

As described below, self-regulation has resulted in unclear and inconsistent policies regarding political ads and microtargeting. These policies can be exploited for pernicious purposes—in addition to microtargeting ads to turn out key voters or influence their views on a candidate or issue, advertisers also use microtargeting to dissuade potential voters seen as unsympathetic to their message.[72] On behalf of the 2016 Trump campaign, Cambridge Analytica purportedly targeted Black voters in swing-states to discourage them from voting.[73] The Russian-government-controlled Internet Research Agency sought to do the same.[74] In a presidential election decided by just 110,000 votes in three swing states,[75] such targeted advertising could have been a critical factor in the outcome. And while it is legal for campaigns to seek to demotivate their opponent's

ads-social-media-stop-microtargeting [perma.cc/UQ5S-33L3].

[69] *Id.*

[70] *Id.*

[71] The state of Washington attempted to require such disclosures, but did not succeed in enhancing transparency across the board. Instead of complying, Facebook, for example, simply stated it would stop running ads subject to the disclosure laws in Washington. *See Facebook Business*: *New Rules for Ads That Relate to Politics in Washington State,* META (Dec. 27, 2018), https://www.facebook.com/business/news/new-rules-for-ads-that-relate-to-politics-in-washington-state [perma.cc/3VYR-B2V6]. For more on ensuing legal challenges to Meta's compliance with Washington law, see *Good Government Groups Defend Washington State Disclosure Law, Facing Opposition from Meta*, CAMPAIGN LEGAL CTR. (Aug. 10, 2023), https://campaignlegal.org/press-releases/good-government-groups-defend-washington-state-disclosure-law-facing-opposition-meta [perma.cc/Q5MR-W7N9].

[72] *See* Janet Burns, *Whistleblower: Bannon Sought to Suppress Black Voters with Cambridge Analytica*, FORBES (May 19, 2018, 12:58 PM), https://www.forbes.com/sites/janetwburns/2018/05/19/241ambridge-analytica-whistleblower-bannon-sought-to-suppress-black-voters/?sh=2a0d881d7a95.

[73] *See* Craig Timberg & Isaac Stanley-Becker, *Cambridge Analytica Database Identified Black Voters as Ripe for 'Deterrence,' British Broadcaster Says*, WASH. POST. (Sept. 28, 2020), https://www.washingtonpost.com/technology/2020/09/28/trump-2016-cambridge-analytica-suppression [perma.cc/GR97-87CJ].

[74] BENKLER ET AL., *supra* note 5, at 240.

[75] Tim Meko, Denise Lu & Lazaro Gamio, *How Trump Won the Presidency with Razor Thin Margins*, WASH. POST*,* (Nov. 11, 2016), https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins [perma.cc/R6VU-9ZA5].

voters,[76] we should strive to safeguard the system against *foreign* efforts to influence American voters through disinformation or intimidation.[77] Even if foreign influence operations were not enough to sway the election in 2016, there is no reason to believe that foreign disinformationists will not double down on such tactics to undermine future elections.

While microtargeting presents real threats, as Chairwoman Weintraub described, it can also play a positive role in elections. This is particularly true in smaller local races. Microtargeting allows candidates to responsibly marshal their resources by targeting ads to their potential constituencies, rather than broader audiences beyond the jurisdiction of the office they seek. Where television or radio ads could be cost-prohibitive, online ads are often within the financial reach of candidates running for local offices.

But completely unregulated microtargeting poses a serious risk to Americans' ability to participate in self-governing activities. As the Supreme Court held in *McIntyre v. Ohio Elections Commission,*

> [i]n a republic where the people are sovereign, the ability of the citizenry to make informed choices among candidates for office is essential, for the identities of those who are elected will inevitably shape the course that we follow as a nation.
> . . . [I]t can hardly be doubted that the constitutional guarantee has its fullest and most urgent application precisely to the conduct of campaigns for political office.[78]

[76] Efforts to make an opponent's supporters less likely to vote can range from legal (if politically sharp-elbowed) tactics, like convincing them that voting is pointless, and their votes do not matter to outright voter suppression and intimidation, which are clearly prohibited by law. *See* 18 U.S.C. § 594. Some of the key policy options analyzed in Part II regarding mandatory searchable databases of online political ads and disclosure of microtargeting would not prevent lawful efforts at dissuading people from voting, but they would serve to shine a light on them. *See infra* Part II. Political operatives would remain free to encourage political opponents not to vote under such regulations, they simply would no longer be free from public scrutiny.

[77] *See* Press Release, U.S. Dep't of Just., Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election (Nov. 18, 2021), https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed [perma.cc/XY2J-JWG3].

[78] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346–47 (1995) (quoting Buckley v. Valeo, 424 U.S. 1, 14–15 (1976) (citations and quotation marks omitted)).

Making *informed* decisions about politics requires that voters be in a position to analyze and assess the information presented. That requires understanding *who* is speaking to them—are they a trustworthy source?—and *why* they are seeing a particular message—were they targeted with a message specifically intended to make them mad or dissuade them from exercising their rights?

As more Americans primarily get their news and political information from social media instead of traditional media, there is a greater chance that the vast majority of the persuasive political content they see will have been targeted to them based on their unique demographic and personal characteristics or internet browsing and purchasing habits.[79] The algorithms applied by social media in microtargeting are meant to exploit and manipulate psychological tendencies, not provide information neutrally to rational decision-makers.[80]

Audiences exposed to a barrage of targeted messages that "play on recipients' fears and . . . activate their tribal loyalties and enmities"[81] are not participating in a vigorous debate of ideas, as John Stuart Mill envisioned, where competing arguments and notions collide, and the truth can overcome falsity through reason and persuasion.[82] Nor are these ideas being exposed to the "competition of the market," as Justice Holmes would put it, where the best test of the truth is that it will prevail in free competition with other ideas.[83] These messages—and their audience—instead end up in information silos, where the listener is not exposed to a range of competing ideas among which they may freely choose.[84] They

[79] *See* Cohen, *supra* note 9, at 647–49.

[80] *See id.* at 649–52.

[81] *See id.* at 652.

[82] *See generally* JOHN STUART MILL, *Of the Liberty of Thought and Discussion*, *in* ON LIBERTY (Andrews U.K. Ltd. 2011) (1859).

[83] *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market.").

[84] Researchers from both the academy and Meta (Facebook's parent company) completed wide-ranging studies on the impact of "filter bubbles" or "information silos" on Facebook users by running a three-month experiment modifying user feeds to reduce the amount of congenial political news (i.e., posts and ads that agreed with the user's existing political worldview) and to increase the amount of other content in their feeds. The results of these studies did not demonstrate a causal link between the amount of congenial political information the user received and their political opinions or level of political polarization. *See* Brendan Nyhan et al., *Like-Minded Sources on Facebook Are Prevalent but Not Polarizing*, 620 NATURE 137, 137–44 (Jul. 27, 2023).

However, the Nyhan study noted that the decline in congenial political content was not correlated with an increase in non-congenial political content. Rather, the decline resulted in more non-political content in the user's feed and potentially neutral (rather than congenial or non-congenial) political content. *See id.* at 138. Beyond the scope of that study, and central to any conceptual framework of instead hear the same message, repeated and amplified, targeted specifically to them based on their personal and psychological characteristics, as discerned through continuous data mining efforts.[85] Good faith actors who disagree with these messages never have the opportunity to provide a rebuttal.

And once a user has received and *engaged* with some disinformation (by liking, replying to, or sharing a post, or clicking on an ad to go to a website), the likelihood they will be directed to more such content increases.[86] Algorithms direct users to content based on patterns of engagement. Because people are more likely to engage with content that angers or upsets them than positive or neutral content,[87] social media platforms frequently suggest false

political debate as a marketplace of ideas, is the conscious exposure of the user to competing ideas—a system in which opposing sides in any debate are aware of the messages their opponents are disseminating and to which audiences, so that they may consciously rebut that message. In other words, they can then issue a countervailing message at that same audience with the specific intention of persuading them to their own position.

There is evidence that simply replacing a few conservative sources in a self-identified conservative user's social media feed with a few liberal ones does not lead to a moderation of the user's viewpoints, but instead reinforces their existing opinions. *See* Christopher Bail et al., *Exposure to Opposing Viewpoints on Social Media Can Increase Political Polarization* 115(37) PROCEEDINGS NAT'L ACAD. SCI. 9216, 9216 (Sept. 11, 2018), https://doi.org/10.1073/pnas.1804840115 [perma.cc/MF3X-QGX2]. By contrast, the results for replacing a few liberal sources with conservative ones in a self-identified liberal user's social media feed were more muted. *See id.*

Of course, the goal of the measures described herein is not to depolarize the electorate, but to help the electorate protect itself from disinformation by alerting them to it and allowing other information sources to counter disinformation in real time. While requirements to disclose microtargeting and maintain Ad Libraries proposed by some of the legislation described in this Article would facilitate the marketplace of ideas, whether that marketplace can actually help inoculate the population against foreign malign influence operations would have to be the subject of further academic study after implementation.

[85] *Understanding the Digital Advertising Ecosystem and the Impact of Data Privacy and Competition Policy: Hearing Before the S. Comm. on the Judiciary,* 119th Cong. 2 (2019) (statement of Dr. Johnny Ryan, Chief Policy Officer, Brave) ("Let me tell you what happens almost every single time you visit a website: data about you is broadcast to tens or hundreds of companies . . . it can include your - inferred - sexual orientation, political views, whether you are Christian, Jewish, or Muslim, etc., whether you have AIDS, erectile disfunction, or bi-polar disorder. It includes what you are reading, watching, and listening to. It includes your location, sometimes right up to your exact GPS coordinates. And it includes unique ID codes that are as specific to you as is your social security number, so that all of this data can be tied to you over time. This allows companies you have never heard of to maintain intimate profiles on you, and on everyone you have ever known.").

[86] Nemr & Gangaware, *supra* note 20, at 34.

[87] *See* Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, WALL ST. J. (May 26, 2020, 11:38 AM), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-

and conspiratorial content to capitalize on the high levels of engagement these posts engender.[88] When microtargeting tools are deployed to intentionally manipulate and misinform the electorate, they pose a risk to the democratic process that we must take seriously.[89]

Different platforms have taken different approaches to microtargeting and political advertisements. In the 2022 midterm election cycle, Twitter, LinkedIn, Pinterest, and TikTok did not allow any political advertisement.[90] Under the new ownership of Elon Musk, a self-proclaimed "free speech absolutist,"[91] Twitter (now known as X) announced in January 2023 that it would begin allowing cause-based political advertising (i.e., issue ads, as opposed to candidate ads).[92] Facebook and Google have hosted and continue to host candidate ads and issue ads from both declared candidates and third-party groups.[93] Facebook allows microtargeting using a broad range of characteristics about the audience, drawn from their behavior on Meta platforms and across the internet, including the content they have viewed or engaged with, as well as their online search and purchasing habits.[94] Yet Facebook does not disclose how ads are microtargeted or what parameters are available to advertisers to use for microtargeting purposes. It also has its own content moderation policies for political advertisements and an ad authorization process to filter out prohibited content before placement.[95]

But prohibited content does not mean all false content. During the 2020 election cycle, Facebook refused to take down political advertisements containing false information, stressing its position that voters should be able to hear directly from candidates.[96] It did, however, prohibit ads with premature claims of election

executives-nixed-solutions-11590507499.

[88] Nemr & Gangware, *supra* note 20, at 34.

[89] BENKLER ET AL., *supra* note 5, at 269.

[90] Dam Hee Kim et al., *Experts Grade Facebook, TikTok, Twitter, YouTube on Readiness to Handle Midterm Election Misinformation*, CONVERSATION (Oct. 26, 2022, 4:14 PM), https://theconversation.com/experts-grade-facebook-tiktok-twitter-youtube-on-readiness-to-handle-midterm-election-misinformation-191249 [perma.cc/6DQ6-JD89].

[91] Elon Musk (@elonmusk), TWITTER (Mar. 5, 2022, 12:15 AM), https://twitter.com/elonmusk/status/1499976967105433600 [perma.cc/D5RV-TNKT].

[92] *See* Sheila Dang, *Elon Musk's Twitter Lifts Ban on Political Ads*, REUTERS (Jan. 4, 2023, 1:47 AM), https://www.reuters.com/business/media-telecom/twitter-expand-permitted-political-advertising-2023-01-03.

[93] *Id.*

[94] *See* Weber, *supra* note 57, at 90.

[95] *Id.* at 96–97.

[96] *See* Nott, *supra* note 7.

victory or which contained misinformation about health and safety issues regarding voting and the COVID-19 pandemic.[97]

In advance of the 2022 election, Facebook issued new guidance for its political ads, stating it would not run political ads in the week before election day.[98] It also would not run ads that discourage people from voting in an election, including ads that portray voting as useless or meaningless, and/or advise people not to vote; call into question the legitimacy of an upcoming or ongoing election; or make premature claims of election victory.[99]

Additionally, Facebook's parent company, Meta, maintains a publicly available Ad Library of the political ads that it runs.[100] The Ad Library includes very limited data about ad targeting, including how much was spent on the ad and the age group, gender, and geographical area it targeted.[101] Facebook allows advertisers to use far more detailed information about the intended audience to microtarget the audience (including users' browsing and engagement habits), but it does not share this data in the Ad Library.[102] Therefore, academic researchers, watchdog groups, political opponents, and the interested public can see the ads that a politician or interest group has run, how much they cost, and the ages, genders, and geographic locations of the people the advertiser wanted to reach. But they cannot see, for example, if the advertiser chose to have the ads shown to a white, rather than a Black, audience. Or if it only wanted self-identified progressives to see the ad. Or if it only sought to target voters with specific interests, educational levels, or internet browsing histories. Meta's maintenance of the Ad Library is entirely voluntary, as there are

[97] *See* Weber, *supra* note 57, at 96; Mike Isaac, *Facebook Moves to Limit Election Chaos in November*, N.Y. TIMES (Sept. 22, 2020), https://www.nytimes.com/2020/09/03/technology/facebook-election-chaos-november.html.

[98] *See* Neil Shrimanker, *Upcoming Restriction Period for US Ads About Social Issues, Elections, or Politics*, META: NEWS FOR DEVELOPERS (Sept. 28, 2022), https://developers.facebook.com/blog/post/2022/09/28/upcoming-restriction-period-for-us-ads (last visited Mar. 4, 2024).

[99] *See Business Help Center: Information on Prohibited Ads Related to Voting and Ads About Social Issues, Elections,* META, https://www.facebook.com/business/help/253606115684173 (last visited Mar. 4, 2024).

[100] *See Ad Library*, META, https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=US&media_type=all (last visited Mar. 4, 2024).

[101] *See, e.g.*, *Meta Ad Library: Beto O'Rourke*, META, https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=US&view_all_page_id=223055747744143&search_type=page&media_type=all (last visited Mar. 4, 2024).

[102] Weber, *supra* note 57, at 97.

currently no federal laws requiring social media platforms to keep such databases or mandating what they should include.[103]

Google also has a published political advertising policy, which it applies to election ads, but not issue ads.[104] To place an election ad on Google, the advertiser must complete a verification form.[105] If the state or locality where the ad will run imposes a disclosure requirement for online ads, Google uses this verification form to automatically generate that information.[106] As discussed *infra,* the FEC does not currently enforce federal disclosure requirements on ads that run online,[107] so there is no corollary federal ad disclosure requirement (though some campaigns still include a "stand by your ad" style disclosure). Google also maintains a voluntary ad library, the Ads Transparency Center, and does not allow any microtargeting of political ads based on factors other than age, gender, and geographic location.[108] Google does allow advertisers, however, to use keywords or contextual ad placement. For example, an ad purchaser could set a particular ad to come up in a search for "Donald Trump," or have the ad run on particular websites.[109] In practice, this means that while your Google search history will not be used to determine what political ads to show you, you may end up seeing ads for Democratic causes or candidates because you visit MSNBC instead of Fox News. Google does not exempt political advertising from the policies that apply broadly to Google ads, including the prohibition on misrepresentations.[110]

3. Sharing and Virality

While bad actors may want to keep some of their advertising and persuasion efforts—such as schemes to depress minority voting—in information silos, away from broader public scrutiny, advertisers want certain information to reach as broad an audience

[103] *But cf.* Honest Ads Act, S.1356, 116th Cong. § 2 (2019) (re-proposed in 118th Congress as Honest Ads Act, S.486, 118th Cong. (2023)).

[104] *See Advertising Policies Help: Political Content, United States (US) Election Ads*, GOOGLE, https://support.google.com/adspolicy/answer/6014595?hl=en#zippy=%2Cunited-states-us-election-ads (last visited Mar. 4, 2024) [perma.cc/9DDW-YDJW].

[105] *Id.*

[106] *See Advertising Policies Help: Election Advertising Verification*, GOOGLE, https://support.google.com/adspolicy/troubleshooter/9973345 [perma.cc/4FNM-TDZY] (last visited Mar. 4, 2024).

[107] *But see* Honest Ads Act, S. 1356, 116th Cong. § 3(9) (2019).

[108] *See Google Ads Transparency Center*, GOOGLE, https://adstransparency.google.com/?region=US [perma.cc/4FNM-TDZY] (last visited Mar. 4, 2024).

[109] *See Advertising Policies Help: Political Content*, *supra* note 104.

[110] *Id.*; Nott, *supra* note 7.

as possible, as quickly as possible. Social media facilitates this as well. Unlike traditional television, radio, or print advertising, the "share" function on social media allows for ads to "go viral," essentially turning the paid-for audience into an amplification system for the message.

Well-designed ads that capture audience attention can generate massive numbers of likes and shares, disseminating the message to an even broader audience than the one the advertiser paid to reach. In addition to "organic virality,"[111] swarms of automated bots and paid trolls or sockpuppets[112] can increase a particular message's audience share. These opaque actors work by spreading messages widely through their own artificially created networks and driving the type of engagement that social media platforms reward with prominent placement in their newsfeeds, thus broadening the audience for a paid ad beyond the initially designed scope.[113] Over a year after the 2016 election, Twitter informed nearly 700,000 of its users that they had unknowingly engaged with—meaning replied to, retweeted, or liked posts from—Russian bot accounts.[114]

Finally, when opponents of an advertising campaign do see the messages, they can unwittingly increase their reach by engaging with those messages. During the 2016 election, high-profile individuals, including former U.S. Ambassador to Russia, Michael McFaul, engaged with Russian trolls and bots posing as Americans, in some instances to debunk their messages.[115] But by engaging with these messages, figures like McFaul would share them with

[111] The Cambridge Advanced Learner's Dictionary & Thesaurus defines "viral" in this context as "used to describe something that quickly becomes very popular or well known by being published on the internet or sent from person to person by email, phone, etc." *Viral*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/viral [perma.cc/4VZP-XQHX] (last visited Mar. 4, 2024). False content is far more likely to "go viral" than true content. On average, a false story reaches 1,500 people six times faster than a factually correct story, with political stories being the content most likely to go viral. *See* Nemr & Gangware, *supra* note 20, at 3.

[112] The questions of what constitutes a "bot" (an automated account, rather than one controlled by a live human) and whether they can or should be regulated are complicated ones that merit greater focus than the scope of this Article allows. For a deeper discussion, see Douglas Guilbeault & Robert Gorwa, *Current Challenges for Bot Policy and Foreign Interference*, in EXAMINING FOREIGN INTERFERENCE IN U.S. ELECTIONS 20–27 (Campaign Legal Ctr. 2018). Additionally, the difference between a "troll" (someone who intentionally antagonizes others online) and a sockpuppet (someone who pretends to be someone else online in order to influence others) is often artificial. *See* BENKLER ET AL, *supra* note 5 at 243.

[113] *See* Cohen, *supra* note 9, at 647–48; Nemr & Gangware, *supra* note 20, at 2.

[114] Ashley Gold, *Twitter: More Than 677,000 U.S. Users Engaged with Russian Troll Accounts*, POLITICO (Jan. 19, 2018, 06:16 PM), https://www.politico.com/story/2018/01/19/twitter-users-russian-trolls-437247 [perma.cc/PX5L-D82F].

[115] MUELLER REPORT, VOL. 1, *supra* note 3, at 27–28.

their own networks, inadvertently expanding their influence. While engaging with disinformation is precisely how the marketplace of ideas theory suggests that we should correct attempts to mislead the public, those who wish to counter disinformation are stymied in their efforts if they cannot readily and reliably identify the source of the disinformation for the audience.

C. Artificial Intelligence

Large Language Model Artificial Intelligence ("LLM AI"), like ChatGPT, will only make the above challenges significantly more complex. Boiled down to its most basic definition, LLM AI is a massive "next-word prediction engine,"[116] trained by reviewing vast quantities of natural language text from Wikipedia entries and news articles to published academic works to social media posts. It can read, translate, and summarize such available texts, and use cues from user prompts to generate a response, predicting what words should come next when producing a coherent text on the designated topic.[117] As a result, LLM AI can respond to user prompts in ways that are difficult—if not impossible—to distinguish from text written by humans.[118]

LLM AI is the technology behind algorithmic chatbots, like OpenAI's ChatGPT, Google's Bard, and Microsoft's Sydney.[119]

[116] Noam Kolt, *Predicting Consumer Contracts*, 37 BERKELEY TECH. L.J. 71, 81–85 (2022); Kevin Roose, *How Does ChatGPT Really Work*? N.Y. TIMES (Apr. 4, 2023), https://www.nytimes.com/2023/03/28/technology/ai-chatbots-chatgpt-bing-bard-llm.html [perma.cc/VS7L-8G5Y].

[117] *See* SAM MANNING ET AL., A RESEARCH AGENDA FOR ASSESSING THE ECONOMIC IMPACTS OF CODE GENERATION MODELS 7 (2022), https://cdn.openai.com/papers/Economic_Impacts_Research_Agenda.pdf [perma.cc/C7H6-N7TM].

[118]*See* Alex Tamkin & Deep Ganguli, *How Large Language Models Will Transform Science, Society, and AI*, STAN. UNIV. HUM.-CENTERED A.I. (Feb. 5, 2021), https://hai.stanford.edu/news/how-large-language-models-will-transform-science-society-and-ai [perma.cc/8ZW6-UGTK].

[119] *See* Kevin Roose, *How Does ChatGPT Really Work*? N.Y. TIMES (Apr. 4, 2023), https://www.nytimes.com/2023/03/28/technology/ai-chatbots-chatgpt-bing-bard-llm.html [perma.cc/XJJ8-T59A]; *Gemini Apps FAQ*, GOOGLE, https://bard.google.com/faq [perma.cc/2GU7-KEB5] (last visited Mar. 4, 2024); David Nield, *How ChatGPT and Other LLMs Work—and Where They Could Go Next*, WIRED (Apr. 30, 2023, 7:00 AM), https://www.wired.com/story/how-chatgpt-works-large-language-model. In fact, Microsoft took Sydney offline for its tendency to produce disturbing and evening threatening responses. The more journalists wrote about Sydney's "bad behavior," the more online content there was on the topic, which Sydney then incorporated into its LLM, reinforcing its problematic behavior. *See* Dr. Gleb Tsipursky, *How the New Microsoft Chatbot Has Stored Its Personality on the Internet*, FORBES (Feb. 27, 2023, 9:50 AM), https://www.forbes.com/sites/glebtsipursky/2023/02/27/how-the-new-microsoft-chatbot-has-stored-its-personality-on-the-internet/?sh=435b5cf4dd9c [perma.cc/CS3U-3P88].

Since ChatGPT-3 was released in November 2022, it has continued to astound users with its ability to quickly produce convincing text in whatever style and on whatever subject the user seeks.[120] The most recent iterations of ChatGPT have passed medical boards,[121] engineering licensing,[122] and bar examinations.[123]

Other AI platforms, like DALL-E and StableDiffusion, can produce realistic audio and video, including audio that sounds like identifiable people.[124] These types of platforms, known as generative AI, have even produced believable episodes of The Joe Rogan Experience[125] and a hit song in the style of Drake and The Weeknd.[126] It's therefore unsurprising that generative and natural language AI have already been used to generate audio and video in political ads.[127] Disinformation researchers are concerned that AI will drive down the cost of generating highly credible disinformation (including fake videos showing people saying things they never said or portraying events that never really happened) to essentially nothing.[128] Current efforts to fight fire with fire and use

[120] Kevin Roose, *How ChatGPT Kicked Off an A.I. Arms Race*, N.Y. TIMES (Feb. 3, 2023), https://www.nytimes.com/2023/02/03/technology/chatgpt-openai-artificial-intelligence.html [perma.cc/X2V3-J69C].

[121] Jennifer Lubell, *ChatGPT Passed the USMLE. What Does that Mean for Med Ed?* AM. MED. ASS'N (Mar. 3, 2023), https://www.ama-assn.org/practice-management/digital/chatgpt-passed-usmle-what-does-it-mean-med-ed [perma.cc/M6E7-GELM].

[122] VINAY PURSNANI ET AL., PERFORMANCE OF CHATGPT ON THE US FUNDAMENTALS OF ENGINEERING EXAM: COMPREHENSIVE ASSESSMENT OF PROFICIENCY AND POTENTIAL IMPLICATIONS FOR PROFESSIONAL ENVIRONMENTAL ENGINEERING PRACTICE (2023), https://arxiv.org/ftp/arxiv/papers/2304/2304.12198.pdf [perma.cc/JM5A-Y2SH].

[123] Debra Cassens Weiss, *Latest Version of ChatGPT Aces Bar Exam with Score Nearing 90th Percentile*, A.B.A. J. (Mar. 16, 2023: 1:59 PM), https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile [perma.cc/S5MZ-K75S].

[124] Sophie Bushwick, *What the New GPT-4 AI Can Do*, SCI. AM. (Mar. 16, 2023), https://www.scientificamerican.com/article/what-the-new-gpt-4-ai-can-do/ [perma.cc/G8WX-GJPP].

[125] The Joe Rogan AI Experience, *Chat GPT - The Joe Rogan AI Experience 001 - Sam Altman - Open AI CEO*, YOUTUBE (Apr. 9, 2023), https://www.youtube.com/watch?v=GhpdkuLHdb8.

[126] *Fake Song Featuring AI of Drake and The Weeknd Goes Viral. Here's Why That's a Problem*, CNN (Apr. 23, 2023), https://www.cnn.com/videos/business/2023/04/23/drake-the-weeknd-ai-song-sarlin-acostanr-contd-vpx.cnn [perma.cc/9DZX-R6X8].

[127] Clay Calvert, *AI Gets Political: How Do We Keep Fake News out of Campaign Ads?* THE HILL (June 13, 2023, 4:00 PM), https://thehill.com/opinion/technology/4046406-ai-gets-political-how-do-we-keep-fake-news-out-of-campaign-ads [perma.cc/Q2T6-BNKW]

[128] Tiffany Hsu & Stuart A. Thompson, *Disinformation Researchers Raise Alarms About A.I. Chatbots*, N.Y. TIMES (June 20, 2023), https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html [perma.cc/D5GA-QZSD].

AI to distinguish computer-generated from human-generated content are unreliable, producing both false positives and negatives.[129]

To date, one of the biggest challenges for foreign adversaries seeking to deploy disinformation has been the difficulty of producing high-quality, credible content that is hard to debunk.[130] Prior Russian disinformation activities have been debunked precisely because, in addition to not being idiomatically correct—many such efforts during the 2016 election cycle were in "pretty poor English"[131]—they often also involved poorly doctored photographs or identifiable actors portraying victims of fake atrocities.[132] It was thus easy to demonstrate they were manufactured.

[129] Keith Collins, *How ChatGPT Could Embed a 'Watermark' in the Text It Generates*, N.Y. TIMES (Feb. 17, 2023), https://www.nytimes.com/interactive/2023/02/17/business/ai-text-detection.html [perma.cc/3Y73-CERX].

[130] For example, after its illegal annexation of Crimea in 2014, Russia spread a false story of Ukrainian troops allegedly crucifying a three-year-old ethnic Russian boy in Slovyansk. Ukrainian journalists quickly debunked the story, pointing to the fact that the town's Lenin Square, where the supposed atrocity took place, did not exist and the "refugee woman" recounting the story to Russian state media was actually the wife of a well-known pro-Russia militant in Ukraine. *See* Jane Wakefield, *TED 2018: Ukrainian Journalist Fights Fake News*, BBC (Apr. 11, 2018), https://www.bbc.com/news/technology-43568238 [perma.cc/4S3Q-H5CU]. A multinational group of journalists launched the website www.StopFake.org specifically to fight this type of disinformation. *See About Us*, STOPFAKE.ORG, https://www.stopfake.org/en/about-us/ (last visited Mar. 4, 2024).

[131] RICHARD STENGEL, INFORMATION WARS: HOW WE LOST THE GLOBAL BATTLE AGAINST DISINFORMATION AND WHAT WE CAN DO ABOUT IT 23 (Atlantic Monthly Press 2019). The difficulty of controlling disinformation in a given country is only compounded when that country comprises numerous linguistic minorities. For example, while English language dis- and misinformation targeting U.S. populations has received much attention, far less has been paid to the same content in Spanish. *See* Stephanie Valencia, *Misinformation Online is Bad in English. But It's Far Worse in Spanish*, WASH. POST (Oct. 28, 2021), https://www.washingtonpost.com/outlook/2021/10/28/misinformation-spanish-facebook-social-media [perma.cc/S4CC-ZMER]; *see also* Steven Lee Myers & Sheera Frenkel, *How Russian Propaganda Is Reaching Beyond English Speakers*, N.Y. TIMES (Aug. 9, 2022), https://www.nytimes.com/2022/08/09/business/russia-propaganda-spanish-social-media.htm [perma.cc/Z5NX-YRD2l].

[132] *See* CHRISTOPHER PAUL & MIRIAM MATTHEWS, THE RUSSIAN 'FIREHOSE OF FALSEHOOD' PROPAGANDA MODEL: WHY IT MIGHT WORK AND OPTIONS TO COUNTER IT 5 (RAND CORP 2016), https://www.rand.org/pubs/perspectives/PE198.html; NATO STRATCOM CTR. OF EXCELLENCE, ANALYSIS OF RUSSIA'S INFORMATION CAMPAIGN AGAINST UKRAINE 13 (2005), https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf [perma.cc/NGN6-DUU4]. In Russian propaganda footage produced after the Euromaidan revolution and the illegal annexation of Crimea,

Artificial intelligence, however, has dramatically reduced these hurdles to creating credible disinformation. Compared to the relatively crude fake videos of just a few years ago, current AI technology now allows disinformationists to create "deep fakes," false videos of actual, identifiable people, that can fool casual observers. In 2022, Russia produced deep fakes of Ukrainian President Volodymyr Zelenskyy purportedly surrendering to the Russians.[133] It is still possible to demonstrate the falsity of such videos.[134] Indeed, the Russian deep fake of Zelenskyy surrendering is choppy, and his head is disproportional to the rest of his body.[135] But the rate at which these technologies are improving is startling,[136] and deep fakes can spread like wildfires across social networks before they are debunked.[137]

While a previous generation of disinformation would have required significant effort and skill to doctor photographs and videos, or to stage fake events using actors, sophisticated AI programs have changed the rules of the game. Now, even users without advanced programming skills can manufacture disinformation at a much greater speed, in different media and multiple languages, which is much harder to identify as fake.[138] This

the same woman was used to play the roles of "Crimean activist," "resident of Kyiv," "soldier's mother," "resident of Odessa," "resident of Kharkiv," "participant of Antimaidan," and "refugee from Donetsk." *Id.*

[133] The Telegraph, *Deepfake Video of Volodymyr Zelensky Surrendering Surfaces on Social Media*, YOUTUBE (Mar. 17, 2022), https://www.youtube.com/watch?v=X17yrEV5sl4 [perma.cc/6MS5-WZ6M].

[134] *See* Matthew Groh et al., *Deep Fake Detection by Human Crowds, Machines, and Machine Informed Crowds*, PROCEEDINGS NAT'L ACAD. SCI., Nov. 25, 2021, https://www.pnas.org/doi/epdf/10.1073/pnas.2110013119 [perma.cc/6CDP-PYSE]. Visit the Northwestern University project, Detect Fakes, to check how good you are at detecting deep fakes. *Detect Fakes*, NW. UNIV. KELLOGG SCH. MGMT., https://detectfakes.media.mit.edu/ [perma.cc/AZL3-ACEK] (last visited Mar. 10, 2024).

[135] The Telegraph, *Deepfake Video of Volodymyr Zelensky Surrendering Surfaces on Social Media*, YOUTUBE (Mar. 17, 2022), https://www.youtube.com/watch?v=X17yrEV5sl4 [perma.cc/6MS5-WZ6M].

[136] *See* Groh et al., *supra* note 134; Catherine Bernaciak & Dominic A. Ross, *How Easy Is It to Make and Detect a Deepfake?*, CARNEGIE MELLON U. SOFTWARE ENG'G INST. BLOG (Mar. 14, 2022), https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/.

[137] *See* Soubik Barari et al., *Political Deepfakes Are As Credible As Other Fake Media and (Sometimes) Real Media*, J. OF POL. (2021), http://christopherlucas.org/files/PDFs/deepfakes.pdf [perma.cc/RB2L-J44R]. The authors' study suggests that "while deepfakes may not be uniquely deceptive, they may still erode trust in media and increase partisan polarization." *Id.*

[138] In addition to the general problem of trying to identify content generated by AI as opposed to human-generated content, ChatGPT can produce content in idiomatically correct Spanish, Chinese, and Arabic, as well as many other languages, allowing foreign bad actors to target U.S. voters who primarily get their information in another language, with more believable disinformation.

will allow disinformationists to generate a much larger quantity of highly credible disinformation, much faster than previously possible, allowing them to better take advantage of the constant feedback from social media advertising about which messages are most successful.

One recent example of this involved fake American news websites created by Kremlin-aligned actors, designed to mimic real local news sources to make false stories appear more legitimate.[139] With names like the New York News Daily and the Miami Chronicle, these sites have presented fake stories, including a fraudulent audio recording, purporting to be of Under Secretary of State Victoria Nuland, discussing whom to select to replace Aleksei Navalny as the next head of the Russian resistance.[140] While not likely to fool a discerning reader, these sites appear to be designed to provide some credence to disinformation stories spread through social media.[141]

Another fraudulent story, suggesting Ukrainian President, Volodymyr Zelenskyy diverted assistance funding to buy himself a pair of mega yachts, was amplified by another Russian-linked fake news site purporting to be based in Washington, D.C.[142] The website, DC Weekly, contains numerous stories from other sources, rewritten with artificial intelligence.[143] The yacht story appears to have fooled numerous Republican members of Congress, who cited the completely debunked claims as reasons not to provide further aid to Ukraine.[144]

Bad actors can also exploit virality on social media to distribute false, AI-created video and audio content using both paid advertising and the amplification effect of influencers and bot armies. As social media platforms have struggled to take down disinformation in languages other than English, speakers of other languages will be particularly susceptible to AI-generated disinformation on these platforms and may be the most vulnerable portions of the U.S. electorate to disinformation efforts.[145]

[139] *See* Steven Lee Myers, *Spate of Mock News Sites with Russian Ties Pop Up in U.S.,* N.Y. TIMES (Mar. 7, 2024), https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html [perma.cc/58KK-F8U8].

[140] *Id.*

[141] *Id.*

[142] Olga Robinson, Shayan Sardarizadeh & Mike Wendling, *How Pro-Russian 'Yacht' Propaganda Influenced US Debate Over Ukraine Aid,* BBC (Dec. 20, 2023), https://www.bbc.com/news/world-us-canada-67766964 [perma.cc/T2BD-435J].

[143] *Id.*

[144] *Id.*

[145] *See* Stephanie Valencia, *Misinformation Online is Bad in English. But It's Far Worse in Spanish*, WASH. POST (Oct. 28, 2021), https://www.washingtonpost.com/outlook/2021/10/28/misinformation-spanish-

While many of the examples listed relate to foreign influence operations with targets other than U.S. elections, we should expect that techniques that have proven effective in Russia's information operations against Ukraine and other European nations[146] will be applied by foreign malign actors trying to influence U.S. domestic affairs, including elections. To date, it is unclear what, if any, actual impact foreign influence operations have had on U.S. elections,[147] but given the rapidly declining costs of interference, the growing tensions between the United States and several of its traditional adversaries,[148] and the potential upside for attackers in undermining citizens' confidence in the validity of U.S. elections,[149] we must take the threat seriously.

II. PROPOSED LEGISLATIVE RESPONSES

Since the 2016 election, there have been several proposals at the federal level to address disinformation in election communications, particularly foreign efforts to target the U.S. electorate. To date, none of these proposed bills has become law. As a result, social media election advertising remains essentially unregulated at the national level. This part will first review

facebook-social-media [perma.cc/S4CC-ZMER]; Steven Lee Myers & Sheera Frenkel, *How Russian Propaganda Is Reaching Beyond English Speakers*, N.Y. TIMES (Aug. 9, 2022), https://www.nytimes.com/2022/08/09/business/russia-propaganda-spanish-social-media.html#:~:text=How%20Russian%20Propaganda%20Is%20Reaching,in%20places%20outside%20the%20West.

[146] *See* Paul & Matthews, *supra* note 132.

[147] *See* BENKLER ET AL., *supra* note 5, at 235–68.

[148] *See generally* H. ARMED SERVICES COMM., 118TH CONG., FINAL REP. OF THE CONG. COMM'N ON STRAT. POSTURE OF THE U.S., (Oct. 2023), https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Strategic-Posture-Committee-Report-Final.pdf [perma.cc/KJ9P-WXHP]. The report describes escalating tensions between the United States and its nuclear peer adversaries, Russia and China, stemming in part from the situations in Ukraine and Taiwan. *See id.* at 7–10. It also addresses threats from non-peer adversaries, Iran and North Korea. *See id.* at 10.

[149] *See generally* Press Release, U.S. Dep't of Just., U.S. Citizens and Russian Intelligence Officers Charged with Conspiring to Use U.S. Citizens as Illegal Agents of the Russian Government (Apr. 18, 2023), https://www.justice.gov/opa/pr/us-citizens-and-russian-intelligence-officers-charged-conspiring-use-us-citizens-illegal [perma.cc/TA8D-ALKB]; Sam Sabin, *Iran is Diving into the Disinformation Wars, Microsoft Says*, AXIOS (May 2, 2023), https://www.axios.com/2023/05/02/iran-disinformation-wars-microsoft); SCOTT W. HAROLD ET AL., CHINESE DISINFORMATION EFFORTS ON SOCIAL MEDIA (2021) (ebook), https://www.rand.org/pubs/research_reports/RR4373z3.html; Seong H. Choi, *North Korea's Provocative and Secret Interventions in South Korean Election*s, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 7, 2022) https://www.csis.org/blogs/new-perspectives-asia/north-koreas-provocative-and-secret-interventions-south-korean [perma.cc/Q4NW-DN49].

legislation implemented at the state level to address election disinformation on social media, and then describe proposals at the federal level to address these same issues on a national basis.

A. Examples of State-Level Attempts to Regulate Social Media Election Advertisements

Numerous states have attempted to regulate social media election advertisements, including using digital ad disclaimer requirements, but this has left an incomplete patchwork of differing laws.[150] Some states, including New York and Washington, have attempted to require social media platforms to maintain a publicly available database of all the political ads they disseminate with key information about the ad's purchaser and intended audience.[151] This subpart provides an overview of these two states' laws, presenting a case study on local responses to social media election advertisements. The guiding theory behind such regulations is that researchers, interest groups, and opposing political candidates would be able to see and understand these messages and potentially offer rebuttals.

New York's Democracy Protection Act of 2018 requires that paid internet and digital political advertisements follow the same disclosure and attribution standards as all other traditional media outlets.[152] It also requires all political committees making independent expenditures (i.e., expenditures not made by a candidate or a national or state political party) to file disclosures identifying the identity of the committee making the expenditures.[153] It requires all persons, groups, or legal entities making independent political expenditures to register with the state as independent expenditure committees, while also prohibiting foreign national governments or their agents from registering as independent expenditure committees.[154] Finally, it requires online platforms that publish political advertisements by independent expenditure committees to obtain copies of the committees' state

[150] *States with Digital Ads Disclaimer Laws*, CAMPAIGN LEGAL CTR., https://campaignlegal.org/sites/default/files/2019-12/Toolkit%20chart%20--%20States%20with%20Digital%20Disclaimer%20Laws%20Graphic%2011-21-19.KB%28CK%29.pdf [perma.cc/ET9U-E8GW] (last visited Mar. 4, 2024).

[151] Katie Paul, *Washington AG Sues Facebook over Political Ads*, REUTERS (Apr. 14, 2020, 3:53 PM), https://www.reuters.com/article/facebook-politics-washington/washington-ag-sues-facebook-over-political-ads-idINL5N2C267L; Jeffrey Trotter, *New Law Requires Full Disclosure for Political Ads on Social Media*, LEGIS. GAZETTE (Apr. 24, 2018), https://legislativegazette.com/new-law-requires-full-disclosure-for-political-ads-on-social-media [perma.cc/8EME-H9R3].

[152] N.Y. ELEC. LAW §§ 14-106, 14-107 (2020).

[153] *Id.* at § 14-106(2).

[154] *Id.* at § 14-107(3).

board of elections registration and to keep those records online and available to the public for at least five years.[155] New York's law does not address microtargeting of advertisements to particular audiences. The New York legislature is currently considering the proposed Democracy Preservation Act, which would go further in preventing foreign-influenced companies from purchasing political advertisements, but the proposed law also does not address microtargeting.[156]

Washington's law requires broader disclosures than New York's, including disclosures about microtargeting of ads in an online, searchable database that is available to the public.[157] But rather than comply with the database requirement, Facebook—the largest social media platform to allow microtargeted political ads—announced it would stop allowing any political advertising in the state.[158] As noted, Facebook maintains an Ad Library and discloses the use of age, gender, and geographic data in microtargeting.[159] The Washington law requiring disclosure of all microtargeting information (including data that Facebook harvests from its users based on information provided voluntarily to Facebook, as well as their browsing histories)[160] compelled Facebook to say they would disallow political ads that "relate[d] to Washington's state or local elected officials, candidates, elections or ballot initiatives," while

[155] *Id.* at § 14-107(5-a).

[156] *See* S. 371, 205th Leg. Sess. (N.Y. 2023).

[157] *See* WASH. REV. CODE ANN. § 42.17A.345 (2019); WASH. ADMIN. CODE § 390-18-050 (2022).

[158] *Digital Political Ads*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 17, 2023), https://www.ncsl.org/research/elections-and-campaigns/digital-political-ads.aspx [perma.cc/P5NJ-M9F7]; *Facebook Business*: *New Rules for Ads That Relate to Politics in Washington State,* META (Dec. 27, 2018), https://www.facebook.com/business/news/new-rules-for-ads-that-relate-to-politics-in-washington-state [perma.cc/AXJ2-YT73]; Eli Sanders, *Facebook Will Halt Political Ad Sales in Washington State by the End of this* Year, THE STRANGER (Dec. 19, 2018, 6:10 PM), https://www.thestranger.com/politics/2018/12/19/37249437/facebook-will-halt-political-ad-sales-in-washington-state-by-the-end-of-this-year [perma.cc/68KU-APZ6].

[159] *See supra* Part I.B.2.

[160] *See* Natasha Singer, *What You Don't Know About How Facebook Uses Your Data,* N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html. In 2022, Apple issued a software update to stop third-party apps (like Facebook) from tracking iPhone users' online behavior without their permission. This change has apparently cost Facebook $10 billion per year. *See* Michael Simon, *Apple's Simple iPhone Alert is Costing Facebook $10 Billion a Year*, *Macworld* (Feb. 3, 2022, 6:54 AM), https://www.macworld.com/article/611551/facebook-app-tracking-transparency-iphone-quarterly-results.html [perma.cc/5KWE-GFCT].

still allowing advertisements about "issues of national importance."[161]

Facebook's stated decision to ban all Washington political ads appeared to eliminate a powerful tool that candidates in local races could have used to get their messages to prospective constituents.[162] When more and more voters get a significant portion of their political news and information from social media, candidates in local races may be shut out of the best possible way to reach their audiences.[163] The state's effort to increase transparency instead seemed to cut off a meaningful avenue for candidates and voters to exchange ideas.

Nevertheless, instead of refusing to run political ads in local and state races in Washington, as Facebook said it would,[164] the platform simply continued to run such ads—without providing the disclosures required under Washington law. The state attorney general sued Meta Platforms (Facebook's parent company) in 2020, alleging repeated violations of state law.[165] Both the state and Meta filed for summary judgment, with Meta arguing that the Washington law was an unconstitutional infringement on its free speech rights.[166] In 2022, Judge North, in King County, Washington, sided with the state on its summary judgment motion, rejecting Meta's First Amendment claim and finding Meta had intentionally violated state law 822 times.[167] The court levied the maximum penalty of $24.6 million against the company.[168]

In the absence of clear federal regulations, the system of platform self-regulation and state-based rules has resulted in different standards in different jurisdictions[169] and across

[161] *See Facebook Business*: *New Rules for Ads That Relate to Politics in Washington State,* META (Dec. 27, 2018), https://www.facebook.com/business/news/new-rules-for-ads-that-relate-to-politics-in-washington-state [perma.cc/AXJ2-YT73].

[162] Weber, *supra* note 57, at 108.

[163] *See* Nott, *supra* note 7.

[164] *See Facebook Business: New Rules for Ads*, *supra* note 161.

[165] Def. Motion Summary Judgment, State of Washington v. Meta Platforms, Inc., No. 20-2-07774-7 (Wash. Super. July 15, 2022), https://www.documentcloud.org/documents/22139465-172_defsmsj.

[166] *Id.*

[167] Order Granting Summary Judgment for the State of Washington, State of Washington v. Meta Platforms, Inc., No. 20-2-07774-7 (Wash. Super. Oct. 6, 2022), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/3944_001.pdf [perma.cc/6AA9-Y5A7].

[168] Judgment, State of Washington v. Meta Platforms, Inc., No. 20-2-07774-7 (Wash. Super. Oct. 26, 2022), https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/Penalties%20judgment.pdf [perma.cc/8SNZ-E6LM].

[169] Weber, *supra* note 57, at 103.

platforms,[170] even though the American public has a general interest in transparency and accountability in political advertising.[171]

As the case of Washington shows, even when jurisdictions impose state-level disclosure requirements in the absence of overarching federal legislation, compliance is hardly guaranteed. Lessons from this case study suggest that federal legislation is the only efficient and tenable way to address the challenges of political advertising on social media. A platform like Facebook, for example, is less likely to respond to a federal requirement for microtargeting disclosure by declaring a ban on most political ads, and then running them anyway without the required disclosures.

B. Proposed Federal Legislative Responses

Five proposed federal laws could, when taken together, provide a coherent (though imperfect) approach to regulating social media advertising. Together, they could significantly reduce the impact of foreign interference, while leaving in place the positive opportunities social media political advertising provides. These proposed bills are the Honest Ads Act ("HAA"),[172] the Protecting Democracy from Disinformation Act ("PDDA"),[173] the DISCLOSE Act,[174] the REAL Political Ads Act ("RPAA"),[175] and the Digital Consumer Protection Commission Act ("DCPCA").[176] While none of these laws is focused exclusively on countering malign foreign influence, each addresses part of the problem.

1. Honest Ads Act ("HAA")

To date, the FEC has not provided guidance for how candidate ad disclosure requirements should apply to online advertisements. As a result, the FEC currently does not strictly enforce the candidate ad disclosure requirement on online ads, in part, because they are often physically smaller than traditional print

[170] *Id.* at 96–97.

[171] Deborah G. Johnson et al., *Campaign Disclosure, Privacy, and Transparency*, 19 WM. & MARY BILL OF RTS. J., 959, 965–66 (2011).

[172] Honest Ads Act, S. 1356, 116th Cong. (2019).

[173] Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. (2020).

[174] Democracy Is Strengthened by Casting Light On Spending in Elections (DISCLOSE) Act of 2021, S. 443, 117th Cong. (2021).

[175] REAL Political Advertisements Act, H.R. 3044, 118th Cong. (2023).

[176] Digital Consumer Protection Commission Act of 2023, S. 2597, 118th Cong. (2023).

ads.[177] The HAA would close this loophole.[178] The proposed law would require the FEC to apply to electioneering advertisements on social media[179] the same type of disclosure and disclaimer requirements that apply to traditional media.[180] The HAA would also prevent the FEC from creating exemptions for candidate ads that run online.[181]

Further, the law would require social media companies to keep databases, or "public political ad files," much the same way broadcasters must under current law.[182] This database requirement would apply to the largest platforms—those with more than fifty million monthly unique users in the United States—and to ads by any purchaser who places $500 or more of advertising on such platforms in a given year.[183] These public political ad files must include (1) the average rate charged for the ad; (2) the candidate's name and office, election, or national legislative issue to which the ad refers; (3) for ads placed on behalf of a candidate, the candidate's name, authorized committee, and treasurer of the committee; and (4) the purchaser of the ad, if not placed with candidate authorization.[184] Finally, the HAA requires social media platforms to make "reasonable efforts" to prevent foreign nationals from purchasing covered political advertisements, either directly or indirectly.[185] The phrase "reasonable efforts" is not defined in the text of the HAA, and would presumably be left to the FEC to interpret and address through the agency rulemaking process.[186]

The HAA would cover all "paid digital communications" on social media.[187] This arguably would include, not only buying ads, but using accounts that one pays others to control (like bots, trolls, and sockpuppets) to amplify those messages, as well as the use of behavioral marketing firms, like Cambridge Analytica, to harvest and use private user data to target advertisements.[188] A broad reading of the HAA such as this would cover the vast majority of

[177] *See* CAMPAIGN LEGAL CTR., THE HONEST ADS ACT 2 (May 2019), https://campaignlegal.org/sites/default/files/2019-05/05-16-19%20HAA%20Issue%20Brief.pdf [perma.cc/K6JY-Y9WX].

[178] *Id.*

[179] Honest Ads Act, S. 1356, 116th Cong. § 6 (2019).

[180] *Id.* at § 7.

[181] *Id.* at § 7(b)(2).

[182] *Id.* at § 8.

[183] *Id.* at § 8(a).

[184] *Id.*

[185] *Id.* at § 9.

[186] For more information on how the FEC administers campaign finance laws and promulgates regulations, which are published each year in Title 11 of the Code of Federal Regulations, see *Regulations*, FED. ELECTION COMM'N, https://www.fec.gov/legal-resources/regulations/ (last visited Mar. 6, 2024).

[187] Honest Ads Act, S. 1356, 116th Cong. § 5 (2019).

[188] BENKLER ET AL., *supra* note 5, at 369.

ways that disinformationists currently reach their targets—not only through direct paid ads, but also through inorganic virality created when bots, trolls, and sockpuppets reshare content on a large scale. But the draft legislation could certainly be more explicit in empowering the FEC to regulate these types of activities. Without a clearer statutory indication that these activities are covered by law, there is no guarantee courts will read the act to permit regulation of such activities, or that the FEC will interpret the law to require such regulation.[189]

Of course, there is no reason to believe foreign intelligence agents seeking to undermine an American election will comply with laws regulating the use of paid accounts to amplify disinformation. For example, the Russian-government-aligned Internet Research Agency and numerous individuals acting on its behalf were indicted for violating existing law,[190] but the likelihood of anyone being tried in the United States for those alleged crimes is essentially nil.[191] But clearly identifying this activity as within the scope of the HAA would give social media platforms firmer justification in undertaking their own efforts to monitor and take down suspicious accounts. Social media platforms already enforce their own terms of service to take down suspicious accounts and take down accounts suspected of engaging in illegal activity.[192] Under Section 230 of the Communications Decency Act of 1996, social media platforms enjoy broad immunity from liability for the content users place on their systems and also retain their immunity from claims of

[189] The Supreme Court's recent decisions relying on a "major questions doctrine," including *West Virginia v. Environmental Protection Agency* and *Biden v. Nebraska* suggest the Court is prepared to strike down regulations by an administrative agency that are not sufficiently delineated in Congress's delegation of power to that agency. In both of these cases, the Court struck down agency regulations on the basis that agency actions with such a "major" policy impact must be the result of a clear congressional delegation of authority. *See* West Virginia v. EPA, 597 U.S. 697, 735 (2022); Biden v. Nebraska, 143 S. Ct. 2355, 2375 (2023). The Court has not, however, clarified what exactly constitutes a "major question." *See generally* Josh Chafetz, *The New Judicial Power Grab*, 67 ST. LOUIS L. J. 635, 649–50 (2023).

[190] Indictment at 2–3, United States v. Internet Research Agency et al., No. 1:18-cr-00032 (D.D.C. Feb 16, 2018), https://www.justice.gov/d9/fieldable-panel-panes/basic-panes/attachments/2018/02/16/internet_research_agency_indictment.pdf [perma.cc/A7V4-KK6V].

[191] *See generally* Spencer S. Hsu, *Justice Department Abandons Prosecution of Russian Firm Indicted in Mueller Election Interference Probe*, WASH. POST (Mar. 16, 2020, 7:29 PM), https://www.washingtonpost.com/local/legal-issues/us-justice-dept-abandons-prosecution-of-russian-firm-indicted-in-mueller-election-interference-probe/2020/03/16/5f7c3fd6-64a9-11ea-912d-d98032ec8e25_story.html.

[192] *See, e.g.*, *Transparency Center: Introduction to the Advertising Standards*, META, https://transparency.fb.com/nl-nl/policies/ad-standards [perma.cc/2FBU-V2KN] (last visited Mar. 6, 2024).

infringing on users' rights when they choose to take down content.[193]

2. Protecting Democracy from Disinformation Act ("PDDA")

The PDDA, in contrast to the HAA,[194] addresses the issue of microtargeting, a tool exploited by foreign actors in the 2016 election.[195] Former Congressman Cicilline's proposed law would ban political microtargeting beyond the use of geographic location (no more specific than ZIP code), age, and/or gender.[196] Social media platforms often overtly collect this information by directly asking their users for it, as opposed to the far more intrusive data that platforms glean by tracking user behavior on both social media platforms and across the internet.[197] The PDDA would allow more targeted advertising only when users affirmatively opt into receiving such communications[198] or when ads are contextually placed.[199] For example, a conservative politician or issue group could choose to place its Google ads on FoxNews.com as opposed to MSNBC.com, but would not be able to have the ads follow a user to other sites based on the user's browsing habits.[200]

[193] 47 U.S.C. § 230.

[194] Microtargeting was not solely used by foreign actors. The Trump campaign's digital efforts on Facebook focused on 13.5 million persuadable voters in sixteen battleground states, with a focus on discouraging them from turning out to vote for Hillary Clinton. *See* BENKLER ET AL., *supra* note 5, at 270. Voters targeted belonged to three key groups: young women, African Americans, and "idealistic white liberals." *See* Elaine Kamarck, *Political Campaigns Are the First Line of Defense in Election Security*, BROOKINGS (Aug. 29, 2019), https://www.brookings.edu/articles/political-campaigns-are-the-first-line-of-defense-in-election-security [perma.cc/TTJ7-4NG3].

[195] Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2(a), (2020).

[196] In 2021, Representative Anna Eshoo of California introduced draft legislation similar to the PDDA, called the Banning Microtargeted Political Ads Act. H.R. 4955, 117th Cong. (2021). It goes beyond the PDDA to prohibit any sort of microtargeting beyond targeting ads to a "recognized place," meaning a state, city, town, census-designated place, congressional district, or other similar unit of general government. Rep. Eshoo's bill would apply to any sort of political advertising (issue ads, electioneering, candidate ads, independent expenditures, etc.) on any online platform that gathered information on more than fifty million users in the prior twelve months. *See id.* at § 2. It would be enforceable by both the FEC and private actors who are improperly targeted by advertisers. *See id.* The constitutional concerns raised by the PDDA, described *infra* in Part III.B, would apply equally to Rep. Eshoo's bill.

[197] Weber, *supra* note 57, at 109–10.

[198] Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2(a), (2020).

[199] *Id.*; Weber, *supra* note 57, at 108.

[200] Weber, *supra* note 57, at 108.

The PDDA would not be limited to ads placed by foreign actors. Rather, it would apply to all political advertisements, including those placed by candidates, political parties, PACs, and super PACs. Its goal is thus broader than merely excluding foreign influence operations. Instead, the bill addresses the problem of disinformation facilitated by information silos, where audiences are targeted for specific reasons beyond their knowledge, regardless of who the speaker is. Described in terms of the marketplace of ideas, the PDDA would work to prevent audiences from being hived off from the broader marketplace and exposed only to a small subset of the possible ideas being debated.

The PDDA would not ban all microtargeting. By allowing microtargeting by age, gender, and geography, the proposed law would allow social media advertising to remain attractive to candidates of more modest means or those running for local offices. And banning microtargeting based on characteristics such as race or religion would reduce the potential for social media advertising to depress turnout among minority voters, or to explicitly target specific racial, religious, or ethnic groups with divisive and extremist content for the purpose of undermining faith in our democratic institutions.[201] It would also increase the cross-section of the population exposed to any given advertisement, expanding opportunities to debate and engage with the messages presented.

But for reasons discussed in Part III.B*,* the prohibitions on certain types of microtargeting (as opposed to required disclosures of microtargeting practices) in the PDDA are not likely to survive strict scrutiny under the Supreme Court's existing First Amendment jurisprudence.[202] Political speech is granted the strongest possible protection under the First Amendment.[203] As such, any governmental regulation of political speech must be narrowly tailored to satisfy a compelling government interest.[204] Government regulation must be the least restrictive form of regulation that would

[201] There is an argument that requiring disclosure of this sort of microtargeting would be an infringement on political speech, but as discussed in Part III, the purpose for granting political speech the broadest possible protection (having a free and open exchange of political ideas) is undermined when advertisers can shield their political speech from scrutiny by the press or their opponents. *See infra* Part III; *see generally* Cohen, *supra* note 9.

[202] *See, e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011) (striking down a state law that limited the sale of physicians' personal information collected by data brokers as an impermissible content-based restriction on speech, even though the purpose of the law was to protect the privacy of physicians' electronically collected personal information).

[203] Meyer v. Grant, 486 U.S. 414, 1894 (1988) ("[T]he speech at issue is 'at the core of our electoral process and of the First Amendment freedoms, an area of public policy where protection of robust discussion is at its zenith.") (citations omitted).

[204] Citizens United v. Fed. Elections Comm'n, 558 U.S. 310, 340 (2010).

achieve the government's compelling purpose. If there is a less restrictive method of achieving that purpose, the government is not free to select a more restrictive regulation.[205] While a blanket prohibition on microtargeting beyond age, gender, and location could help prevent the intentional targeting of specific populations for political disinformation (which should be considered a compelling government interest), it is unlikely to survive strict scrutiny because it is such a sweeping regulation that would dramatically affect how online advertising can be directed at relevant audiences. In Part III.B, this Article considers the strengths of arguments for and against the PDDA's microtargeting limitations under the First Amendment and also considers how less restrictive alternatives, including requiring disclosure of all microtargeting efforts or requiring platforms to allow users to opt out of receiving microtargeted ads, would likely fare.

3. REAL Political Advertisements Act ("RPAA")

The RPAA was introduced in the House in May 2023 by Representative Yvette Clark of New York, not long after the Republican National Committee launched the first-ever political advertisement including AI-generated content.[206] The bill's companion in the Senate is sponsored by Senators Klobuchar, Booker, and Bennet.[207] The RPAA would require clear and conspicuous disclosure of any content in a political ad that was generated by AI, whether print, audio, or video.[208] It would apply this requirement to broadcast, internet, or digital communications, including advertisements on online platforms.[209]

While not specifically addressed by the RPAA, its requirement that AI-generated content be conspicuously labeled could be assisted by a broader requirement that AI-generated content include a digital "watermark" in its code, identifying it (regardless of format) to other artificial intelligence as content that was created by AI, thus allowing for easier AI content detection.[210] Numerous scholars have debated the potential for requiring indelible digital watermarks as a method of policing AI-generated content against various types of misuse (like misattribution, deep fakes,

[205] McCutcheon v. Fed. Elections Comm'n, 572 U.S. 185, 197 (2014).
[206] Matt Novak, *GOP Releases First Ever AI-Created Attack Ad Against President Biden,* FORBES (Apr. 25, 2023, 3:01 PM), https://www.forbes.com/sites/mattnovak/2023/04/25/gop-releases-first-ever-ai-created-attack-ad-against-president-biden [perma.cc/AT3E-Q4ZX].
[207] REAL Political Advertisements Act, S. 1596, 118th Cong. (2023).
[208] *Id.* at § 4(a).
[209] *Id.* at § 3.
[210] JOHN KIRCHENBAUER ET AL., A WATERMARK FOR LARGE LANGUAGE MODELS (June 6, 2023), https://arxiv.org/pdf/2301.10226.pdf [perma.cc/RJX2-6X3E].

disinformation, etc.).[211] While it would not be a fool-proof approach, it could provide a significant tool for identifying AI-generated content, as required by the RPAA, thus facilitating enforcement and giving it some regulatory "teeth."

Digital watermarks in AI-generated content would also allow platforms and researchers to identify such content, even when the creator failed to adhere to the proposed disclosure laws. If platforms can successfully identify foreign sources of political advertising and undisclosed AI-generated content, they could potentially blunt the negative impacts of AI-generated foreign disinformation. A both/and approach to required disclosure of an ad purchaser's identity and whether it was produced using artificial intelligence (with required watermarking as a critical backstop) would be the most appropriate method of addressing the problems posed by AI-generated disinformation, as neither one alone would be sufficient to prevent abuse.

4. Digital Consumer Protection Commission Act ("DCPCA")

The DCPCA was introduced primarily as a means to regulate large technology businesses.[212] But the bill identifies and addresses national security concerns, as well.[213] Title V of the proposed bill would require the dominant technology platforms to be owned or operated by American corporate entities or persons.[214] It also requires that no director of a dominant technology platform be a citizen of a foreign adversary and that ownership interest in dominant technology platforms by citizens of foreign adversaries be strictly limited.[215] Platforms would not be allowed to store or process U.S. citizens' data in restricted countries.[216] Operators of dominant technology platforms would be required to identify "bots," including their countries of origin.[217] These provisions, while not specifically addressing foreign influence in U.S. elections,

[211] Keith Collins, *How ChatGPT Could Embed a 'Watermark' in the Text it Generates,* N.Y. TIMES (Feb. 17, 2023), https://www.nytimes.com/interactive/2023/02/17/business/ai-text-detection.html [perma.cc/CM3H-FDH2].

[212] Press Release, Sen. Elizabeth Warren, Warren, Graham Unveil Bipartisan Bill to Rein in Big Tech (July 27, 2023), https://www.warren.senate.gov/newsroom/press-releases/warren-graham-unveil-bipartisan-bill-to-rein-in-big-tech [perma.cc/NNQ9-WFWM].

[213] The stated purpose of the DCPCA is "[t]o amend the Clayton Act to establish a new Federal commission to regulate digital platforms, including with respect to competition, transparency, privacy, and national security." Digital Consumer Protection Commission Act of 2023, S. 2597, 118th Cong. (2023).

[214] *Id.* at § 2501.

[215] *Id.*

[216] *Id.* at § 2502.

[217] *Id.* at § 2503.

would make it more difficult for adversaries who have control or significant access to dominant platforms currently used in the United States (such as the Chinese-owned social media platform, TikTok), to exploit that data for influence operations.

While not directly addressed as a national security concern, the DCPCA would also require platforms to allow users to opt out of algorithmic recommendations and would prohibit targeted advertising based on data collected across different platforms.[218]

The requirements to identify foreign bots and allow individuals to opt out of cross-platform targeted ads and algorithmic recommendations would provide users some defenses against being unknowingly funneled into an information silo. But requiring the user to affirmatively exercise their opt-out rights would not achieve the broader disclosure goal of ensuring users know the source of political speech intending to influence their behavior.

5. Democracy is Strengthened by Casting Light on Spending in Elections Act of 2023 ("DISCLOSE Act")

The final piece of proposed legislation, the DISCLOSE Act, addresses several campaign disclosure concerns, several of which are relevant here. The other proposed responses discussed—the HAA, the PDDA, the RPAA, and the DCPCA—do not address the issue of "dark money," funds spent by groups like super PACs or 501(c)(4)s, which are currently not subject to requirements to disclose the identity of their funders.[219] They also do not address foreign-influenced corporate entities, whose ability to engage in political speech is lightly regulated.[220] So long as foreign actors are able to "launder" their political influence operations through such entities, the salutary provisions of the HAA and PDDA cannot adequately address the threat posed by foreign interference. As the

[218] *Id.* at § 2415.

[219] In *Americans for Prosperity Found. v. Bonta,* the Supreme Court struck down a California law requiring registered charities to disclose to the state their major donors, even though these donor lists were shielded from public disclosure. 141 S. Ct. 2373, 2389 (2021). While the Court has repeatedly upheld disclosure requirements for election-related activity, most recently in *Citizens United*, it is likely super PACs will attempt to use the *Bonta* holding to argue against the constitutionality of any requirement to disclose their major contributors. For a discussion on the open questions raised by *Bonta* and what it could mean for the future of campaign finance disclosure regimes, see Sara L. Neier, *Americans for Prosperity Foundation v. Bonta: Protecting Free Speech and its Implications for Campaign Finance Disclosures*, 2 FORDHAM L. VOTING RTS. & DEMOCRACY F. 148 (2023), https://ir.lawnet.fordham.edu/vrdf/vol2/iss1/5.

[220] Michael Sozan, *Fact Sheet: Stopping Political Spending by Foreign-Influenced U.S. Corporations*, CTR. AM. PROGRESS (May 3, 2022), https://www.americanprogress.org/article/fact-sheet-stopping-political-spending-by-foreign-influenced-u-s-corporations.

DOJ's indictment of the Internet Research Agency readily demonstrates, Russian state actors and their agents went to great lengths to pretend to be Americans to target their American audience.[221] HAA's requirement that platforms take reasonable steps to prevent foreigners from purchasing political advertisements will be effectively toothless so long as advertisers can use entities like super PACs and issue advocacy groups to hide their identities.

Senator Sheldon Whitehouse's DISCLOSE Act addresses these very issues. Introduced in every Congress since the Supreme Court decided *Citizens United* in 2010, the DISCLOSE Act would require super PACs and other groups spending on election activities to disclose all of their donors who contribute over $10,000 in a given year.[222] It would also prevent the use of shell entities to obscure donors by requiring that the entities' true owners be disclosed.[223] And it includes a "Stand By Every Ad" provision, requiring covered entities to disclose the top funders paying for each ad.[224] While not specifically aimed at foreign state actors, these disclosure requirements would make it harder for foreign actors to hide their status to influence campaigns.

The DISCLOSE Act would also create an audit and reporting requirement, tasking the FEC to determine the extent to which there was illicit foreign election interference aimed at spreading disinformation among rural, minority, or other populations after each election.[225] It would also ensure that federal prohibitions on foreign election interference apply to state and local elections, referenda, and ballot initiatives.[226] Finally, it would prohibit establishing corporations to conceal election contributions and donations by foreign nationals.[227]

6. Additional Legislative Responses to Consider

As discussed in Part IV, Congress should also consider including in any legislative efforts to tackle foreign disinformation the roles that various government agencies should play in this task.

[221] Indictment at 3–4, United States v. Concord Mgmt. & Consulting LLC, No. 18-cr-00032 (D.D.C. Feb. 16, 2018).

[222] Democracy is Strengthened by Casting Light on Spending in Elections Act of 2023, S. 512, 118th Cong. § 201 (2023); *see* Press Release, Sen. Sheldon Whitehouse, Whitehouse, Cicilline Reintroduce Disclose Act to End Corrupting Influence of Dark Money in American Democracy (Feb. 17, 2023), https://www.whitehouse.senate.gov/news/release/whitehouse-cicilline-reintroduce-disclose-act-to-end-corrupting-influence-of-dark-money-in-american-democracy [perma.cc/2K2U-S7UP].

[223] *Id.*

[224] *Id.* at § 401.

[225] *Id.* at § 102

[226] *Id.* at § 103.

[227] *Id.* at § 105.

The HAA, PDDA, RPAA, and DISCLOSE ACT lay out the role of the FEC in addressing disinformation in social media advertising—but they do not address the fact that most subject matter expertise about foreign influence operations rests elsewhere in the federal government. Cooperation and coordination among the Department of Justice, Department of Homeland Security, the State Department, and other entities is essential to successfully identifying foreign disinformation operations. Congressional involvement in setting the strategy for this interagency cooperation can help avoid confusion and provide for necessary oversight.

While we should expect that malign foreign actors will adapt to whatever means we choose to block their influence over our electoral politics, the provisions of these proposed bills, when combined, provide an excellent starting point to address the threat of foreign influence operations aimed at sowing discord and undermining our democracy.

III. FIRST AMENDMENT IMPLICATIONS

When efforts to regulate political speech are challenged in court, they typically trigger strict scrutiny.[228] This review requires the government to show that its efforts to regulate political speech are narrowly tailored to achieve a compelling government interest.[229] Additionally, limitations on speech that are not "viewpoint neutral"—in other words, regulations of speech based on the point of view expressed—are also highly suspect and unlikely to survive judicial review.[230]

The types of regulations described in the legislation proposed in Part II.B can be grouped into three broad categories: (1) disclosure requirements, (2) restrictions on microtargeting and algorithmic political advertising, and (3) efforts to exclude foreign actors from political communications. For the reasons explained in this part, both disclosure requirements and efforts to exclude foreign actors from election-related speech are likely to survive judicial review. Prohibitions on types of microtargeting or algorithmic political advertising, however, are likely to be struck down, both because they are content-based restrictions, and therefore not viewpoint-neutral, and because they are overbroad.

[228] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010) (holding that limitations on campaign spending by private groups were subject to strict scrutiny and thus would survive only if narrowly tailored to a compelling government interest).

[229] *Id.*

[230] *See* Reed v. Town of Gilbert, 576 U.S. 155, 163–64 (2015) (holding that any regulation of speech based on its substantive content is subject to strict scrutiny).

A. First Amendment Jurisprudence: The Strongest Possible Protections for Political Speech

Political speech has long been considered to be at the heart of the First Amendment and enjoys the highest possible protection from regulation.[231] As such, while blatantly false speech may be outright banned in a commercial context,[232] it will receive robust First Amendment protection in the political context.[233]

Courts apply strict scrutiny when reviewing efforts to regulate political speech, requiring that the government use "narrowly tailored" approaches to advance a "compelling" government interest.[234] The types of laws that have failed to meet this exacting standard are numerous and varied, and include efforts to regulate how much candidates[235] and private groups[236] can spend on election advertising. Election activity that is clearly prohibited in other advanced democracies, including making false claims in a political ad, is protected by the U.S. Constitution.[237]

But not all regulation of political speech is doomed. Courts have upheld individual contribution limits to particular candidates.[238] They have also upheld bans on electioneering at polling places and communications that constitute voter intimidation.[239] And courts, including the Supreme Court, have

[231] *See* Meyer v. Grant, 486 U.S. 414, 425 (1988).

[232] *See, e.g.*, Illinois *ex rel.* Madigan v. Telemarketing Assocs., Inc., 538 U.S. 600, 606 (2003) (holding that fraudulent charitable solicitation is unprotected speech).

[233] *See* Susan B. Anthony List v. Driehaus, 814 F.3d 466, 473–74 (6th Cir. 2016) (upholding a district court decision to strike down an Ohio law criminalizing false statements made in political campaigns because it swept in all false political speech, not just speech that could undermine election integrity).

[234] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010).

[235] *See* Buckley v. Valeo*,* 424 U.S. 1, 57 (1971) (striking down federal limits on how much candidates could raise and spend).

[236] *See generally Citizens United*, 558 U.S. at 310 (striking down limits on corporate independent political spending).

[237] *See Susan B. Anthony List*, 814 F.3d at 473–74. An issue that has not yet arisen, but which may test American courts' commitment to protecting false political speech, is the issue of "deep fakes," false videos that are extremely realistic and difficult to debunk. If a campaign generates and disseminates a video of its political opponent saying something he did not say, but which is indistinguishable from a genuine video, it would dramatically undermine the functioning of the marketplace of ideas. It is possible that existing libel law can address this potential problem, but that would require private, after-the-fact enforcement. *See generally* Jessica Ice, *Defamatory Political Deepfakes and the First Amendment*, 70 CASE W. RESERVE L. REV. 417 (2019).

[238] *See Buckley*, 424 U.S. 1 at 7 (discussing legal limits on individual contributions to a candidate in each election cycle).

[239] Burson v. Freeman, 504 U.S. 191, 211 (1992) (upholding bans on campaigning at polling places and bans on communications that amount to voter intimidation as narrowly tailored to achieve a compelling government interest in protecting the right to vote, and thus constitutional under the First Amendment).

consistently upheld disclosure requirements for political speech, even while striking down other means of campaign finance regulation.[240] Indeed, the Court has relied on Justice Brandeis's premise that "[s]unlight is said to be the best of disinfectants" to justify disclosure laws.[241] While the Supreme Court has noted that some anonymous political speech is protected by the First Amendment,[242] courts have routinely found that the government's interest in ensuring the public knows the relationship between candidates and advertisement sponsors is a compelling one that allows for disclosure rules.[243]

Except for the PDDA's ban on microtargeting,[244] the above-described legislative remedies are not only well-targeted at the problem, but they are also likely to withstand judicial scrutiny under the standard that political speech is entitled to the broadest possible protection to ensure a competitive marketplace of ideas.[245] Courts have long recognized the salutary effects of disclosure laws in political speech. Knowing the identity, and therefore the interests, of the speaker helps an audience properly analyze and weigh political speech.[246] As Justice Brandeis put it, the solution to the problem of "falsehoods and fallacies" is not "enforced silence"—it is more speech.[247]

Indeed, disclosure has often been cited by the Supreme Court as a proper alternative to more significant restrictions on political

[240] *See, e.g.*, *Buckley*, 424 U.S. 1; McConnell v. Fed. Election Comm'n, 540 U.S. 93 (2003), *overruled by* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010); *Citizens United*, 558 U.S. 310; SpeechNow.org v. Fed. Election Comm'n, 599 F.3d 686 (D.C. Cir. 2010).

[241] *Buckley*, 424 U.S. at 67 (quoting LOUIS BRANDEIS, OTHER PEOPLE'S MONEY 62 (Nat'l Home Libr. Found. ed. 1933).

[242] *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (striking down a state law ban on anonymous leafletting).

[243] *See, e.g.*, Fed. Election Comm'n v. Pub. Citizen, 268 F.3d 1283, 1287 (11th Cir. 2001) (upholding candidate authorization disclosure requirements under a strict scrutiny analysis).

[244] As stated above, Congresswoman Eshoo's Banning Microtargeted Political Ads Act—which would ban all microtargeting of political ads, except to a recognized geographic area, or to individuals who expressly opt into targeted political ads—creates the same First Amendment concerns as the PDDA. *See* Banning Microtargeted Political Ads Act of 2021, H.R. 4955, 117th Cong. (2021).

[245] Red Lion Broad. Co. v. Fed. Commc'n Comm'n, 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail . . .").

[246] *See* SpeechNow.org v. Fed. Election Comm'n, 599 F.3d 686, 698 (D.C. Cir. 2010) ("[T]he public has an interest in knowing who is speaking about a candidate and who is funding that speech . . .").

[247] Whitney v. California, 274 U.S. 357, 377 (1927), *partially overruled by* Brandenburg v. Ohio, 395 U.S. 444 (1969) (Brandeis, J., concurring) ("If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.").

speech. In *McCutcheon v. FEC*, writing for the majority on the issue of limits on total expenditures, Chief Justice John Roberts held:

> [D]isclosure of contributions minimizes the potential for abuse of the campaign finance system. Disclosure requirements are in part "justified based on a governmental interest in provid[ing] the electorate with information" about the sources of election-related spending. They may also deter actual corruption and avoid the appearance of corruption by exposing large contributions and expenditures to the light of publicity. Disclosure requirements burden speech, but—unlike the aggregate limits—they do not impose a ceiling on speech. For that reason, disclosure often represents a less restrictive alternative to flat bans on certain types or quantities of speech.[248]

While *McCutcheon* addressed disclosure as an alternative to limitations on campaign finance, the logic applies equally well here. The disclosure rules in the proposed legislation described in Part II.B impose no ceilings on speech by requiring disclosure of the speaker's identity, the identification of foreign funders, or the use of artificial intelligence in political speech. Rather, they provide the electorate with important information about who is speaking and why. They also assist in reducing the likelihood or even the appearance of corruption.

Further, disclosure rules in this context have another important goal beyond the context of campaign contributions—by requiring disclosure of the details regarding paid communications and who they targeted, the marketplace of ideas Justice Holmes so forcefully defended in his *Abrams* dissent can work properly.[249] If the remedy for false speech is not censorship, but more speech, that remedy can only work if interested speakers are aware of potential falsehoods they can then seek to counter. Otherwise, allowing speakers to make their claims to large, diffuse, but strategically targeted audiences, away from public scrutiny, would thoroughly undermine the marketplace of ideas.

[248] McCutcheon v. Fed. Election Comm'n, 572 U.S. 185, 223 (2014) (citations omitted).

[249] "[T]he ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . " Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). The dissent "stands as one of the central organizing pronouncements for our contemporary vision of free speech." Lee C. Bollinger, THE TOLERANT SOCIETY 18 (1986).

A final justification for disclosure rules that would require making the public aware of the substance of communications, who paid for them, and to whom they were directed is that such rules can help deter online voter intimidation and harassment. Communications intended to harass, threaten, or intimidate a voter out of exercising the franchise are not only unlawful, but they can also be criminal.[250] While many of the foreign influence operations aimed at depressing voter turnout in the 2016 and 2020 presidential elections did not rise to the level of voter intimidation, some did.[251] And states and the federal government already prosecute individuals who engage in voter intimidation efforts through robocalls,[252] tweets,[253] and emails.[254]

For instance, one of the best-documented examples of voter intimidation during the 2020 election was the case of robocalls made to mainly African-American voters in Michigan and four other states by two conservative operatives, warning the recipients against voting in that year's presidential election.[255] The robocall falsely told recipients that they could be subject to arrest, debt collection, and even mandatory forced vaccination if they attempted to vote.[256] The perpetrators of the calls, Jacob Wohl and Jack Burkman (who helpfully included their real names in the robocalls placed to voters),[257] pled guilty to telecommunications fraud in Ohio in October 2022, and were sentenced to probation, fines, and 500 hours

[250] *See* 18 U.S.C. §§ 594, 241; 52 U.S.C. § 20511(1). Laws criminalizing voter intimidation may be justified on the grounds that an actor's First Amendment rights do not extend to preventing another from exercising *their* core political rights. Given the racist history of voter intimidation before passage of the Voting Rights Act in 1965, voter intimidation was and is a critical civil rights concern. *See* Voting Rights Act of 1965, § 11(b).

[251] *See* Press Release, U.S. Dep't of Just., Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election (Nov. 18, 2021), https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed [perma.cc/4Z74-UZD6].

[252] Ryan J. Foley, *Conservative Hoaxers Face Charges over False Voter Robocalls*, ASSOCIATED PRESS (Oct. 1, 2020, 7:38 PM), https://apnews.com/article/election-2020-technology-arrests-michigan-voting-rights-5f035e2a68394f9765d9c0d500538d94 [perma.cc/28MS-AHZG].

[253] Press Release, U.S. Dep't of Just., Social Media Influencer Douglass Mackey Convicted of Election Interference in 2016 Presidential Race (Mar. 31, 2023), https://www.justice.gov/usao-edny/pr/social-media-influencer-douglass-mackey-convicted-election-interference-2016 [perma.cc/873V-S2SB].

[254] *See* Press Release, U.S. Dep't of Just., *supra* note 77.

[255] Foley, *supra* note 252.

[256] *Id.*

[257] The audio recording of the robocall is available at: *(703) 795-5364 is a Political Robocall*, NOMOROBO (Aug. 26, 2020), https://www.nomorobo.com/lookup/703-795-5364?recording=CAee7daeeadd7759e923ec881092e29d04 [perma.cc/QEW4-QC72].

of registering voters in Washington, D.C.[258] Both men are also facing felony charges in Michigan stemming from the fake robocall scheme.[259]

Expanding disclosure rules to cover social media advertising will make it more likely that bad actors intending to exploit this avenue of communication with voters will not engage in criminal voter intimidation because of the increased likelihood of being caught. Social media platforms charged with determining and cataloging the identities of political ad purchasers would be required to reject potential ads that violate the disclosure requirements, reducing the likelihood that disinformationists could avoid detection.

B. Possibilities for Regulating Microtargeting

1. Is Microtargeting Speech?

Current First Amendment jurisprudence suggests that what constitutes speech must be broadly defined.[260] For example, speech includes video games,[261] computer programs,[262] encryption software,[263] and search engine results.[264] But unlike entire games or software programs (which as of this writing, are still generally written by human authors) search engine results are typically

[258] Emily Olson, *They Ran a Voter Suppression Scheme. Now They're Sentenced to Register Voters*, NPR (Dec. 1, 2022, 2:38 PM), https://www.npr.org/2022/12/01/1140096697/jacob-wohl-jack-burkman-robocalls-ohio-sentence [perma.cc/DS2Y-QBPE].

[259] *See* Press Release, Mich. Dep't of Att'y Gen., Oral Arguments Held Before Michigan Supreme Court in Voter Intimidation Case, People v. Burkman and Wohl (Nov. 9, 2023), https://www.michigan.gov/ag/news/press-releases/2023/11/09/oral-arguments-held-before-michigan-supreme-court-in-voter-intimidation-case [perma.cc/RH3L-XYJ6].

[260] Stuart M. Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445, 1453–54 (2013).

[261] Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 790 (2011) (holding that video games constitute expressive speech protected by the First Amendment).

[262] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445–47 (2d Cir. 2001) (finding that "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code" and that "[c]omputer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer.").

[263] Bernstein v. Dep't of Just., 176 F.3d 1132, 1141 (9th Cir. 1999) ("[E]ncryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine.").

[264] Search King, Inc. v. Google Tech., Inc., No. 02-1457, 2003 WL 21464568, at *3–4 (W.D. Okla. May 27, 2003) (holding that search engine results that rank pages according to their relative significance to the search queries are constitutionally protected expressions of opinion, covered by the First Amendment).

generated by an algorithm, rather than by a human's particularized decision-making, meaning they do not have a direct human author. Nevertheless, search results that "curate" the content users see are protected speech.[265] The theory behind this is that since they are designed to return results that are "most helpful" to the user[266] they constitute speech. It is information that is sent, received, and capable of being understood, even if not authored by a person.[267]

Microtargeting advertisements—whether created by humans selecting a particular audience based on demographic information gathered from internet histories or by machine learning performing the same task—are also likely to be considered a form of protected speech. As with search engine results, microtargeting allows substantive information (i.e., the political message) to be communicated. The act of choosing whom to speak to is either speech in and of itself, or it is a useful aid in communicating to an audience.[268] As described above, microtargeting can be used to direct issue ads to individuals for whom the information is particularly relevant.

As the Supreme Court has repeatedly held, the right to free speech in the political context is both the right of the speaker to be heard and the right of the audience to hear the message.[269] Prohibiting microtargeting would therefore constitute interference with both the right of the speaker to tailor their message to improve its impact on the political conversation, and the right of recipients to hear information that they might find useful in making political decisions, including for whom to vote. Under First Amendment jurisprudence, such a prohibition would trigger strict scrutiny—it would require the government to show that there is no less burdensome method to achieve the compelling government interest in preventing voter deception than allowing voters to combat the purportedly misleading speech with counter-speech, thus allowing

[265] *Id.*

[266] *See* Eugene Volokh & Donald M. Falk, *First Amendment Protection for Search Engine Search Results*, GOOGLE (Apr. 20, 2012), http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf [perma.cc/H7XN-F7MB].

[267] Benjamin, *supra* note 260, at 1461.

[268] Talia Bulka, Comment, *Algorithms and Misinformation: The Constitutional Implications of Regulating Microtgargeting*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1107, 1122–23 (2022).

[269] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339 (2010) ("The right of citizens to inquire, to hear, to speak, and to use information . . . is a precondition to enlightened self-government and a necessary means to protect it."); Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[T]he Constitution protects the right to receive information and ideas."); Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853, 867 (1982) ("[T]he right to receive ideas is a necessary predicate to the *recipient*'s meaningful exercise of his own rights of speech, press, and political freedom.").

the marketplace of ideas to function. As the Supreme Court has noted, it is the "rare case" that survives this exacting scrutiny.[270]

The next subpart examines arguments in favor of the constitutionality of the PDDA's microtargeting ban and, conversely, arguments that it is unlikely to withstand strict scrutiny, given the Supreme Court's current jurisprudence on political speech.

2. Arguments in Favor of the Constitutionality of Microtargeting Bans

The strongest arguments in favor of the constitutionality of the PDDA's restrictions on microtargeting include that it neither precludes any particular message, nor prevents anyone who wishes to receive microtargeted ads from opting into such advertising. Individuals would still be able to choose to receive ads based on their race, political opinion, interests, or browsing habits. But for those who want access to a broader marketplace of ideas, curtailing microtargeting would help preserve that marketplace, allowing competing speakers to see which messages are reaching an audience and to then reach out to that same audience with a counter-message.[271]

Microtargeting that seeks to obscure what is being said, by whom, and to whom threatens the purpose of the First Amendment. Advocates for microtargeting bans would argue that they are narrowly tailored efforts to curtail this conduct and uphold the compelling government interest in a robust marketplace of political ideas.[272] As Commissioner Ellen Weintraub explained,

> [these companies] are targeting ads in very small slices to people, making sure [they're] almost custom-designed for you. At the same time, anyone who disagrees is likely to be getting a different ad set . . . There's no opportunity for what we call

[270] *See* Burson v. Freeman, 504 U.S. 191, 211 (1992) (plurality opinion) (upholding Tennessee's ban on polling place electioneering under a strict scrutiny analysis, recognizing that "it is the rare case in which we have held that a law survives scrutiny.").

[271] *See* Melody Hahm, *Why 'Micro-Targeting' Is a Problem for Elections*, YAHOO! FINANCE (Jan. 22, 2020), https://finance.yahoo.com/news/fec-commissioner-ellen-weintraub-on-micro-targeting-elections-211638687.html [perma.cc/R6KF-DVGT].

[272] Red Lion Broad. Co. v. Fed. Commc'n Comm'n, 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail . . ."); *see also* Ellen L. Weintraub, *Opinion, Don't Abolish Political Ads on Social Media. Stop Microtargeting*, WASH. POST (Nov. 1, 2019), https://www.washingtonpost.com/opinions/2019/11/01/dont-abolish-political-ads-social-media-stop-microtargeting [perma.cc/7ZEG-87SM].

> counterspeech, for someone to come out and say, "wait a minute, that's not right, there's another take on that," or "there's other information that you really ought to hear in order to make an informed judgment."[273]

Advocates for microtargeting bans would also argue the PDDA does not completely foreclose the possibility of microtargeting ads, given customers can still opt into receiving them.[274] The opt-in provision causes the PDDA to differ markedly from the total bans on the use of collected private data that the Supreme Court has struck down.[275]

Additionally, online microtargeting differs substantially from in-person audience selection in important ways that bolster arguments for different regulations. When a candidate gives a speech to a group of veterans or a neighborhood association, the audience is aware that the speaker has chosen to speak to them because of their characteristics or membership in a particular group. In other words, they have the contextual information necessary to understand the speaker's message may be tailored to them. But when it comes to microtargeting of online ads, the audience is generally unaware of the extent of the information that has been collected on them and how that information was used to target them.[276] Without this information, they are at a significant disadvantage in their efforts to analyze and weigh the arguments presented. Indeed, ordinary social media users, who typically lack knowledge of how the newsfeeds and advertisements they see are curated based on their online activity, may have no idea that they have been hived off into a dead end within the broader marketplace of ideas, only exposed to certain messages meant to reaffirm their existing belief, to demoralize them, or to frighten them, or play on base emotions.[277]

3. Why Microtargeting Bans Will Likely Be Held Unconstitutional

Arguments for banning microtargeting may focus on the important interest of protecting people's private data—which they

[273] *See* Hahm, *supra* note 271.

[274] *See* Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2 (2020).

[275] *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 557 (2011) (finding a Vermont law violated the First Amendment by prohibiting the sale of personal data electronically collected from physician prescribers).

[276] *See* Ira S. Rubenstein, *Voter Privacy in the Age of Big Data*, WIS. L. REV. 861, 891 (2014).

[277] *See* BENKLER ET AL., *supra* note 5, at 273.

may not even know is being harvested from their online activity—from exploitation. But even if this were accepted as a compelling government interest, an outright ban on using an individual's private data to direct communications to them—as opposed to a regime requiring disclosure or giving people the right to opt out of such targeted communications and data usage—is likely to be struck down for lack of narrow tailoring.

First Amendment jurisprudence in other contexts suggests as much. Even in commercial speech, where greater government regulation is allowed to suppress false or misleading speech, or to protect consumer interests,[278] the Supreme Court has struck down efforts to limit data mining and other potential invasions of individuals' privacy interests when the laws impinged upon speech. For example, in *Sorrell v. IMS Health*, the Court struck down a Vermont law restricting the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors.[279] The purpose of the law was to prevent data miners from using that information to invade individuals' privacy interests.[280] But the Supreme Court held that "[s]peech in aid of pharmaceutical marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment. As a consequence, Vermont's statute must be subjected to heightened judicial scrutiny. The law cannot satisfy that standard."[281]

In *Sorrell*, the speech in question was aimed at advancing a commercial purpose, not a political one, meaning it was afforded a lower level of protection than political speech would be. In judicial review terms, this means the Court applied intermediate, rather than strict, scrutiny.[282] Intermediate scrutiny requires the state to show "that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest."[283] The activity in question, mining and selling individual user data to determine individual doctors' prescribing patterns, was held to be expressive conduct. The Court held Vermont's regulation on this expressive conduct was content based[284] (because the state

[278] *See* Va. State Bd. of Pharm. v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 770–72 (1976) (striking down a state law prohibiting public-facing prescription drug price advertisements, but noting that, in the context of commercial speech, government is empowered to prohibit false, misleading, or deceptive speech: "The First Amendment, as we construe it today does not prohibit the State from insuring that the stream of commercial information flow cleanly as well as freely.").

[279] *Sorrell*, 564 U.S. at 557.

[280] *See id.* at 572.

[281] *Id.* at 557.

[282] *See id.* at 570.

[283] *Id.* at 572 (citing Bd. of Trs. SUNY v. Fox*,* 492 U.S. 469, 480–81, (1989)).

[284] For a summary of how content-based and viewpoint-based regulations are treated differently under First Amendment jurisprudence, and key case law on the

disagreed with the content, rather than, say, with the time, place, or manner of the speech), subjecting it to heightened scrutiny.[285] The state's blanket ban on such conduct therefore violated the Free Speech Clause, even under the less exacting intermediate scrutiny standard.

Given the outcome in *Sorrell*, where the Court found a Free Speech interest in gathering individuals' private data for *marketing* purposes in a commercial context,[286] it is difficult to see how a blanket ban on microtargeting using individuals' personal data to direct *political* speech could survive strict scrutiny.

The PDDA's opt-in regime, which would allow microtargeting when users expressly agree to it, differentiates it from a total ban and could therefore theoretically save the ban on microtargeting ads. But this regime remains problematic because it is not the "least restrictive means" available to the government.[287] Instead of requiring users to opt into microtargeting—a less restrictive way of achieving the government's purpose—the law could require them to opt out of microtargeting.[288] This is especially true if the hypothetical opt-out provision applies to all advertisements, not just political ones.

matter, see Lindsay Hemminger, Note, Americans for Prosperity Foundation v. Bonta*: The Dire Consequences of Attacking a Major Solution to Dark Money in Politics*, 81 MD. L. REV. 1007, 1019 (2022) ("Content-based laws, which single[] out specific subject matter for differential treatment, are subject to strict scrutiny. Viewpoint-based laws, which attempt to regulate one side of a political controversy, are also subject to strict scrutiny. Where a regulation is based on the content of the speech or the viewpoint of the speaker, the Court scrutinizes it more carefully to ensure that communication has not been prohibited 'merely because public officials disapprove of the speaker's views.") (citations omitted).

[285] *See Sorrell*, 564 U.S. at 565.

[286] Professor Balkin compellingly argues that the Free Speech Clause has become a shield for evading legitimate regulation of economic activity and that whether speech should receive the fullest level of protection under the Free Speech Clause should turn on whether that speech is intended to influence public viewpoints on an issue (whether political, social, or cultural), allowing for greater regulation of speech and expressive conduct that is not meant to influence public viewpoints. *See* Balkin*, supra* note 25, at 1217. Despite the conceptual appeal of this interpretation, it is not likely to result in a swift change in First Amendment jurisprudence. To be successful, any effort to combat foreign disinformation operations must be implemented on a shorter timeframe than would be possible if we must first seek to change how the Supreme Court views the First Amendment. That is why this Article frames the constitutionality test within the existing First Amendment jurisprudence.

[287] *See* U.S. West, Inc. v. Fed Commc'n Comm'n, 182 F.3d 1224, 1239 (10th Cir. 1999) (striking down an "opt-in" requirement when the government could have instead used an "opt-out" requirement, commenting that "[e]ven assuming that telecommunications customers value the privacy of [the regulation], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy").

[288] *See id.* at 1238–39.

As noted above, burdening political speech more substantially than other forms of speech amounts to a content-based restriction, which creates its own First Amendment problems. The Supreme Court defines content-based restrictions as "those that target speech based on its communicative content" or that "appl[y] to particular speech because of the topic discussed or the idea or message expressed."[289] In the context of political speech, content-based restrictions must satisfy strict scrutiny.[290] The PDDA and BMPAA both single out microtargeting in the context of political speech, making the restrictions content-based.[291] Preventing political advertisers from choosing their audience through microtargeting is likely to be struck down because it constitutes a content-based restriction (i.e., it applies to political speech, but not commercial speech).[292] Additionally, the stated reasons for restricting microtargeting in both proposed bills demonstrate that the government opposes the substantive message of political microtargeting.[293] That was also the case in *Sorrell*, where the Supreme Court held that restricting data mining because of government disagreement with that expressive conduct constituted a content-based restriction.[294] Indeed, even the DCPCA's restriction on using cross-platform data for algorithmic advertising is in jeopardy of being struck down under the decision in *Sorrell.*[295]

On the other hand, opt-out regimes that apply to all types of digital data collection and use without differentiation based on the substance of the information communicated already exist and can serve as a model for efforts to combat disinformation. The California Consumer Data Privacy Act, which went into effect in 2018, allows California residents to opt out of the collection and use

[289] Reed v. Town of Gilbert, 576 U.S. 155, 162–65 (2015).

[290] *See id.* at 164–65 (finding that the town's sign code, which subjected political signs to greater restrictions than other signs, was content based on its face and thus subject to strict scrutiny).

[291] *See* Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2 (2020); Banning Microtargeted Political Ads Act of 2021, H.R. 4955, 117th Cong. § 2 (2020).

[292] *See Reed*, 576 U.S. at 165 ("A law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of 'animus toward the ideas contained' in the regulated speech.") (quoting Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 429 (1993).

[293] *See* Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2 (2020); Banning Microtargeted Political Ads Act of 2021, H.R. 4955, 117th Cong. § 2 (2021).

[294] *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 565–66 (2011).

[295] *See id.* at 557. *But see* Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'n Comm'n, 555 F.3d 996, 999–1000 (D.C. Cir. 2009) (upholding agency regulation requiring telecommunications carriers to obtain consumer consent through an opt-in process before sharing private consumer data with third parties).

of their private data.[296] Given California's successful implementation of the act, a national law accomplishing the same objectives is likely to survive any constitutional challenges,[297] whereas an outright ban on microtargeting (or an opt-in regime) remains likely to be struck down.

Opponents of a ban on microtargeting could also easily point to disclosure laws as a less restrictive means for the government to achieve its interest in preventing the spread of disinformation in non-transparent ways that would prevent opponents from engaging with and countering the disinformation. Given that, it is difficult to see how the type of microtargeting bans endorsed by the PDDA or Representative Eshoo's Banning Microtargeted Political Ads Act[298] could survive strict scrutiny.

Although critics of approaches that either place the onus on the user to opt out of microtargeting or limit regulations to mere disclosures (rather than prohibitions) can certainly argue these methods are less likely to be effective than an outright ban on microtargeting, current First Amendment jurisprudence makes the more sweeping approaches not viable.

[296] *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (2018).

[297] While there is not yet well-developed case law regarding the constitutionality of the CCPA on First Amendment grounds, in other contexts, courts have upheld laws regarding the use of consumers' private data that can be analogized to the CCPA. The "Customer Proprietary Network Information" (CPNI) rules codified in Section 222 of the Communications Act require telecommunications carriers to protect the confidentiality and proprietary information of other carriers and of customers. 47 U.S.C. § 222. The D.C. Circuit found that the federal government's interests in protecting consumers from unwanted (and potentially dangerous) communications was sufficient to require affirmative consumer consent using an opt-in requirement before a carrier could share consumer data under the commercial speech test. *See* Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'n Comm'n, 555 F.3d 996, 1002 (D.C. Cir. 2009).

Commentators have also previously questioned whether the CCPA violates the dormant commerce clause by placing a burden on out-of-state actors in commerce. *See* Kiran K. Jeevanjee, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U. L. REV. F. 75, 75 (2020). But the Supreme Court's decision in *National Pork Producers Council v. Ross*, upholding California regulations on commercial pork production, strongly suggests that out-of-state actors cannot rely on the fact that a state's regulations burden their commercial activity as a basis for constitutional challenge when that regulation does not differentiate between in-state and out-of-state actors and is connected to a legitimate state interest. 598 U.S. 356, 369 (2023).

[298] *See supra* text accompanying note 193.

4. Why Changing the First Amendment Paradigm for Disinformation Campaigns Will Fail

While some commentators suggest that the current First Amendment paradigm is ill-suited to address challenges such as international disinformation campaigns,[299] the Supreme Court's application of strict scrutiny to any efforts to regulate political speech is unlikely to be meaningfully relaxed. To restore a more comprehensive marketplace of ideas to social media, it is neither necessary nor practical to change the robust level of protection that political speech enjoys under American jurisprudence. Supreme Court precedent aggressively protects political speech from content regulation on the theory that it is not the place of government to moderate what candidates can say to their prospective constituents.[300] Those constituents have a *right* to hear the information and make up their minds.[301] Even outright lies in political speech are typically protected from government efforts to censor them, when they are not defamatory or otherwise actionable, because government actions to suppress such speech cannot survive strict scrutiny.[302] But the types of regulations described in Part II.B—disclosure rules, including for microtargeting based on personal data or opt-out rights for consumers—are precisely the sorts of regulations that should survive even strict scrutiny.

A new free speech jurisprudence for algorithmic speech, as some have called for,[303] would require a departure from existing

[299] *See* Cohen, *supra* note 9, at 651; Annie C. Hundley, *Fake News and the First Amendment: How False Political Speech Kills the Marketplace of Ideas*, 92 TUL. L. REV. 497, 513–14 (2017); Balkin, *supra* note 25, at 1215; Kimberley Rhum, *Information Fiduciaries and Political Microtargeting: A Legal Framework for Regulating Political Advertising on Digital Platforms*, 115 NW. L. REV. 1829, 1833–34 (2021).

[300] *See* McCutcheon v. Fed. Election Comm'n, 572 U.S. 185, 191–92 (2014) ("[T]he First Amendment 'has its fullest and most urgent application precisely to the conduct of campaigns for political office.'") (quoting Monitor Patriot Co. v. Roy, 401 U.S. 265, 272 (1971)).

[301] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 339 (2010) ("The right of citizens to inquire, to hear, to speak, and to use information . . . is a precondition to enlightened self-government and a necessary means to protect it."); Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[T]he Constitution protects the right to receive information and ideas."); Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853, 867 (1982) ("[T]he right to receive ideas is a necessary predicate to the *recipient*'s meaningful exercise of his own rights of speech, press, and political freedom.").

[302] *See, e.g.*, Susan B. Anthony List v. Driehaus, 814 F.3d 466, 473 (6th Cir. 2016); 281 Care Comm. v. Arneson, 766 F.3d 774, 784 (8th Cir. 2014); Rickert v. State Pub. Disclosure Comm'n, 168 P.3d 826, 848–49 (Wash. 2007) (en banc) (applying strict scrutiny and finding unconstitutional Washington's political false-statements law that required proof of actual malice, but not defamatory nature).

[303] *See generally* Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495 (2013).

precedent[304] and is contrary to the current direction of Supreme Court cases on political speech.[305] Given that such a change in the Supreme Court's jurisprudence on political speech is highly unlikely, it is more appropriate to focus efforts on crafting solutions to the problem that are likely to pass constitutional muster.

C. What About AI?

Regulating artificial intelligence used in political advertising raises its own challenges.[306] The Federal Elections Commission recently deadlocked on whether it has the ability to regulate the use of deepfakes or other deceptive material generated by AI in political advertising.[307] Several of the commissioners told the press they did not believe the Commission currently has the power to regulate such advertisements and would need Congress to expand its jurisdiction for the FEC to regulate such ads.[308]

The RPAA would not ban the use of artificial intelligence in ads but would require its disclosure.[309] As noted above, disclosures are more likely to survive strict scrutiny than other efforts to limit political speech.[310] But disclosure laws in the context of AI-generated content are essentially toothless unless such content is

[304] *See* Benjamin Stuart Minor, *Algorithms and Speech*, 161 U. PA. L. REV. 1445, 1473 (2013).

[305] *See, e.g.*, Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010) (taking a very narrow view of the government's legitimate interest in limiting political spending only to prevent quid pro quo corruption, striking down limits on independent campaign expenditures, and affirming the rights of corporations to expend unlimited resources in political campaigns as core protected political speech).

[306] On October 30, 2023, the Biden Administration signed a sweeping executive order on the safe, secure, and trustworthy development and use of artificial intelligence. *See* Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence. While it touches on disinformation, it focuses on several other concerns, including consumer privacy, combatting fraud, protecting critical infrastructure, and ensuring that AI does not have dramatic negative impacts on labor. *See id.*

[307] *See* Minutes of an Open Meeting of the Federal Election Commission, FED. ELECTION COMM'N 3 (June 22, 2023), https://www.fec.gov/updates/june-22-2023-open-meeting/ [perma.cc/H2NT-Z569].

[308] *See* Daniela Altimari, *FEC Deadlocks on Whether to Govern Deepfake Campaign Ads*, ROLL CALL (June 22, 2023), https://rollcall.com/2023/06/22/fec-deadlocks-on-whether-to-govern-deepfake-campaign-ads [perma.cc/D6MM-BTGV].

[309] *See* REAL Political Advertisements Act, H.R. 3044 § 4 (2023).

[310] *See* Buckley v. Valeo, 424 U.S. 1, 67 (1976), *overruled by* Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010) ("Sunlight is said to be the best of disinfectants[.]") (quoting LOUIS BRANDEIS, OTHER PEOPLE'S MONEY 62 (Nat'l Home Libr. Found. ed. 1933)).

readily identifiable. But foreign disinformationists are highly unlikely to adhere to such niceties.

AI watermarking is an effective means to add teeth to a prohibition on undisclosed AI-generated content.[311] The White House has obtained a voluntary commitment from AI industry leaders to add these watermarks to guard against danger.[312] But as the technology spreads, relying on voluntary compliance becomes more and more risky. Requiring watermarking is a potential solution, but may itself run into First Amendment problems as a form of "compelled speech."[313]

This area is ripe for further research, including whether a watermark could be properly characterized as a content-neutral (meaning not limited to political speech, but to all AI-generated content) "time, place, or *manner*" restriction.[314] In addition to being content-neutral, such restrictions must be narrowly tailored to achieve a significant government interest. Here, a government requirement to disclose AI-generated content would be necessary to allow individuals to discern the trustworthiness of the information provided and investigate its claims. Time, place, and manner restrictions also must leave ample alternative channels for the speaker to convey their message. As watermarking can be required in a content-neutral manner, and does not place a significant burden on the communication of any message, human- or AI-generated, it is a good candidate for a permissible time, place, and manner restriction on speech. But as we are in uncharted territory in

[311] *See generally* JOHN KIRCHENBAUER ET AL., A WATERMARK FOR LARGE LANGUAGE MODELS (2023), https://arxiv.org/pdf/2301.10226.pdf [perma.cc/X29R-GT9F].

[312] *See Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, WHITE HOUSE (Jul. 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai [perma.cc/5DN5-XA92].

[313] *See* W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 633 (1943) (striking down a requirement that students stand and say the pledge of allegiance at school as an unconstitutional requirement that students declare a belief). Courts have also struck down state laws compelling individuals to display a particular ideological statement on their private property. *See, e.g.*, Wooley v. Maynard, 430 U.S. 705, 707 (1977). But in a professional or commercial setting, courts have upheld compelled disclosures of factually accurate information. So long as the disclosure requirement is reasonably related to the state's interest in preventing consumer deception, it will be upheld as constitutional under current jurisprudence. Nevertheless, the right of a commercial speaker not to be compelled to divulge accurate information about its products or services is not a fundamental right. *See* Zauderer v. Office of Disciplinary Couns., 471 U.S. 626, 651, 652 n.14 (1985); Milavetz, Gallop, & Milavetz v. United States, 559 U.S. 229, 232 (2010) (requiring advertisements for certain debt relief businesses to disclose that the services offered include bankruptcy assistance).

[314] *See* Ward v. Rock Against Racism*,* 491 U.S. 781, 789–90 (1989).

attempting to govern AI-generated speech and, as Justice Kagan has admitted, the Court is not "the nine greatest experts on the internet,"[315] it is essentially impossible to predict at this point how the Supreme Court would approach a mandatory AI watermarking law.

D. Foreign Actors Can Be Completely Excluded from Acts of Democratic Self-Governance

While any regulations that apply generally to political speech will be subject to strict scrutiny, courts have routinely upheld blanket prohibitions on foreign actors participating in activities of democratic self-governance.[316] The theory behind this is the government may exclude foreign citizens from activities "intimately related to the process of democratic self-government."[317] Excluding noncitizens from participation in the democratic political process is part of the government's obligation to preserve the basic conception of a political community.[318] As such, regulations banning foreign actors from purchasing political ads,[319] requiring platforms to take reasonable measures to prevent such purchases,[320] and prohibiting the use of corporations to conceal election contributions and donations by foreign nationals[321] should easily withstand judicial

[315] *See* Amy Howe, "*Not, Like, The Nine Greatest Experts on The Internet": Justices Seem Leery Of Broad Ruling on Section 230*, SCOTUSBLOG (Feb. 21, 2023), https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230 [perma.cc/MJT2-WK2N].

[316] *See, e.g.*, Bluman v. Fed. Election Comm'n, 565 U.S. 1104 (2012) (unanimously affirming, without an opinion, a D.C. District Court decision allowing a blanket prohibition on campaign contributions from lawfully present foreigners who were not U.S. citizens or lawful permanent residents); Bernal v. Fainter, 467 U.S. 216, 220 (1984) (noting that the Court has often upheld blanket prohibitions on the grounds that they advance a compelling state interest, despite invalidating the law at issue); Gregory v. Ashcroft, 501 U.S. 452, 456 (1991) (holding unconstitutional under the Equal Protection Clause a provision of Missouri's state constitution requiring appointed judges to retire upon reaching seventy years of age); Cabell v. Chavez-Salido, 454 U.S. 432, 435–36 (1982) (upholding a California law requiring deputy probation officers and other peace officers to be U.S. citizens); Foley v. Connelie, 435 U.S. 291, 292–93 (1978) (upholding a New York state law barring foreign citizens from serving as police officers); Perkins v. Smith, 370 F. Supp. 134, 136, 138 (D. Md. 1974), *aff'd* 426 U.S. 913 (1976) (upholding a Maryland state law barring foreign citizens from serving as jurors, holding that "[s]uch service may appropriately be limited to citizen members of the political community").

[317] *See Bernal*, 467 U.S. at 220.

[318] *See Foley*, 435 U.S. at 295–96.

[319] Democracy Is Strengthened by Casting Light On Spending in Elections Act of 2023, S. 512, 118th Cong. §§ 101–05 (2023).

[320] Honest Ads Act, S. 1356, 116th Cong. (2019).

[321] Democracy Is Strengthened by Casting Light On Spending in Elections Act of

scrutiny under standards previously applied.[322] But because of the risk of foreign actors posing as domestic ones to evade bans, these measures must be paired with robust disclosure requirements to have any hope of serving as a meaningful check on foreign disinformation operations.[323]

IV. WHOLE OF SOCIETY RESPONSES

On the legal front, the most effective first step toward countering foreign disinformation is via congressional action as described in Part II.B. Overcoming political opposition to enact these laws will most likely be difficult,[324] but it will also be insufficient to address the problem. New rules and tools are required to address foreign disinformation. But operationalizing the effort will require a broad, multilayer effort best categorized as "whole of society." While it is beyond this Article's scope to fully describe the contours of executing an effective effort to combat foreign influence on elections, this Part will briefly sketch out the high level of coordination necessary for achieving this goal.

Most of the draft legislation described above identifies the FEC as the agency with responsibility for addressing the problem.[325] And while there is no doubt that the FEC, as the primary agency charged with regulating federal elections, must take the lead in

2023, S. 512, 118th Cong. § 105 (2023).

[322] Bluman v. Fed. Election Comm'n*,* 800 F. Supp. 2d 281, 285 (2011), *aff'd* 565 U.S. 1104 (2012).

[323] That domestic actors would also need to disclose their microtargeting activity and use of paid accounts to amplify their messages should not be viewed as a collateral consequence of attempting to limit foreign disinformation. Requiring domestic actors to make such disclosures has its own salutary effects and the government has a compelling interest in providing this information to the electorate so voters can properly assess the information they receive. *See* SpeechNow.org v. Fed. Election Comm'n, 599 F.3d 686, 698 (D.C. Cir. 2010) ("[T]he public has an interest in knowing who is speaking about a candidate and who is funding that speech.").

[324] Press Release, Sen. Sheldon Whitehouse, Whitehouse Blasts Republican Blockade of the Disclose Act (Sept. 22, 2022), https://www.whitehouse.senate.gov/news/release/whitehouse-blasts-republican-blockade-of-the-disclose-act [perma.cc/HD7S-F9NE]. Additionally, despite repeatedly calling for more ad transparency regulation, Facebook has lobbied against passage of the bipartisan Honest Ads Act. *See* Heather Timmons & Hanna Kozlowska, *Facebook's Quiet Battle to Kill the First Transparency Law for Online Political Ads*, QUARTZ (Mar. 22, 2018), https://qz.com/1235363/mark-zuckerberg-and-facebooks-battle-to-kill-the-honest-ads-act [perma.cc/2ZHG-QWZY].

[325] *See, e,g.*, Democracy Is Strengthened by Casting Light On Spending in Elections Act of 2023, S. 512, 118th Cong. §§ 201, 203, 205 (2023); Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2 (2020); Honest Ads Act, S. 1356, 116th Cong. § 8 (2019); Require the Exposure of AI-Led Political Advertisements Act, H.R. 3044, 118th Cong. §§ 2, 4, 5 (2023).

developing and enforcing regulations required by proposed legislation, it has neither the subject matter expertise nor the resources to actually detect foreign disinformation in real time, identify its source, or counter its impact. As the DISCLOSE Act proposes, the FEC may be called upon to audit election cycles to determine the impact of foreign disinformation after the fact.[326] Undoubtedly, that is a critical part of any response to disinformation, as are enforcement actions against actors who violate standards for foreign-sponsored political ads, disclosure requirements,[327] or microtargeting limitations.[328] But post-election enforcement cannot disarm disinformation campaigns in time to preserve the integrity of an election when it matters.

New legislation and additional responsibilities for the FEC are merely the first step in addressing the disinformation problem. Once rules and authorities are in place, the government will need to deploy high levels of interagency, intergovernmental, and public-private coordination to detect, alert, and counter foreign electoral disinformation operations. These efforts will require buy-in from social media platforms and academic researchers to identify and raise the alarm about foreign disinformation and will depend upon greater international cooperation with other governments facing the same threats. They will also require limited, but critical, involvement of agencies not normally involved in domestic affairs.

Foreign bad actors have not limited their efforts to national elections. The architect of the quixotic CalEXIT initiative—a failed ballot measure to have California secede from the union—was, in fact, an American citizen living in Russia, supported by Russian political and media outlets.[329] Russian internet trolls also targeted the Women's March to undermine its efficacy as a movement.[330] The federal government must be prepared to alert the public, the media, and state and local governments as it becomes aware of these efforts. Otherwise, the longer disinformation is allowed to flourish without challenge, the more likely it will trigger the sort of cascade

[326] Democracy Is Strengthened by Casting Light On Spending in Elections Act of 2023, S. 512, 118th Cong. § 102 (2023).

[327] Honest Ads Act, S. 1356, 116th Cong. § 8 (2019).

[328] Protecting Democracy from Disinformation Act, H.R. 7012, 116th Cong. § 2 (2020).

[329] John Sepulvado, *From His Home in Russia, #Calexit Leader Plots California Secession*, KQED (Dec. 13, 2016), https://www.kqed.org/news/11217187/from-his-home-in-russia-calexit-leader-plots-california-secession [perma.cc/87AC-BFEW].

[330] Ellen Barry, *How Russian Trolls Helped Keep the Women's March out of Lockstep*, N.Y. Times (June 21, 2023), https://www.nytimes.com/2022/09/18/us/womens-march-russia-trump.html [perma.cc/FK5B-ND7U].

effect that enhances its staying power and makes it harder to discredit.[331]

Independent researchers taking advantage of the political ad database contemplated by the HAA[332] will be critical to identifying specific instances of disinformation, as will the platforms themselves, as there are no actors better positioned to identify suspicious accounts and suspected bots.[333] The federal government should consider appropriate methods to encourage cooperation across platforms and researchers so that they may identify and alert to specific instances of disinformation.[334] Platforms should publish their standards for determining disinformation and the steps they will take to remove fake accounts and disinformation.[335]

[331] *See* Cohen, *supra* note 9, at 647–48.

[332] Honest Ads Act, S. 1356, 116th Cong. § 8 (2019).

[333] Nathaniel Persily & Joshua A. Tucker, *How to Fix Social Media? Start With Independent Research*, BROOKINGS INST. (Dec. 1, 2021), https://www.brookings.edu/articles/how-to-fix-social-media-start-with-independent-research [perma.cc/3365-PEVQ].

[334] Governmental efforts to work with platforms to identify and counter disinformation have been stymied by legal efforts to block such cooperation, including a lawsuit brought by a number of states with Republican Attorneys General against the Biden administration. *See* Missouri v. Biden, No. 22-CV-01213, 2023 WL 4335270, at *1 (W.D. La. July 4, 2023). Judge Terry A. Doughty initially granted plaintiffs' request for a preliminary injunction, which would have had broad, sweeping repercussions for governmental efforts to identify and publicize disinformation on social media. *See id.* Judge Doughty's order was then stayed by the Fifth Circuit Court of Appeals, pending the federal government's appeal of the injunction. The Fifth Circuit then modified the ruling and injunction. *See* Missouri v. Biden, 83 F.4th 350, 398 (5th Cir. 2023) (upholding the central reasoning of Judge Doughty's decision, but loosening the restrictions on the government's conduct). On October 20, 2023, the Supreme Court granted the Biden administration's request for a stay of the Fifth Circuit's order and writ of certiorari. *See* Murthy v. Missouri, 144 S. Ct. 7, 7 (2023). Given Judge Doughty's ruling was not supported by controlling legal precedent, its broad sweep and its central holding—that the government is forbidden from discussing certain topics with social media platforms—is in tension with Supreme Court precedent recognizing the *government's* right to speak. *See* Pleasant Grove City v. Summum*,* 555 U.S. 460, 468 (2009) ("A government entity may exercise this same freedom to express its views when it receives assistance from private sources for the purpose of delivering a government-controlled message."). It is unlikely the federal government will find itself completely precluded from addressing disinformation on social media platforms. Regardless of how the Supreme Court resolves the matter, opponents of the government's efforts to combat disinformation—whether driven by a civil libertarian perspective or by concerns about a partisan dimension to counter-disinformation efforts—are likely to continue in their efforts to prevent the government from identifying and publicizing certain speech as disinformation, whether it relates to vaccines, elections, or any other contentious topics.

[335] The Digital Advertising Alliance has prepared a set of "Self-Regulatory Principles for Digital Political Advertising." APPLICATION OF THE SELF-REGULATORY PRINCIPLES OF TRANSPARENCY & ACCOUNTABILITY TO POLITICAL ADVERTISING, DIGITAL ADVERTISING ALLIANCE (May 2018),

Government agencies with experience monitoring and responding to foreign disinformation will also need to lend their expertise to the effort. Not only are agencies such as the Department of Justice's National Security Division, the State Department, the Department of Homeland Security, and the various elements of the intelligence community[336] more familiar with identifying and responding to Russian active measures (including information operations),[337] but these agencies also maintain connections across the globe with allied and partner governments experiencing disinformation campaigns against their own countries.

Despite its foreign policy remit, the State Department has a strategic interest in countering disinformation. The State Department's first strategic objective is to mobilize international coalitions against global challenges posing a threat to American security, including disinformation campaigns.[338] Likewise, the Department of Homeland Security's focus on cybersecurity and protecting critical information infrastructure is implicated by the threat of disinformation. DHS's Cybersecurity and Infrastructure Security Agency's Mis-, Dis-, and Malinformation (MDM) team is charged with building national resilience to MDM and foreign influence activities.[339] One of its objectives is to assist state, local, and tribal governments to prepare for and respond to threats of MDM from foreign and domestic sources targeting electoral processes run by these governmental bodies.[340]

https://aboutpoliticalads.org/sites/politic/files/DAA_files/DAA_Self-Regulatory_Principles_for_Political_Advertising_May2018.pdf [perma.cc/QCX4-YGAE]. While self-regulation is insufficient to meet this challenge, there is no question that platforms establishing appropriate internal standards and practices is critical to minimizing the negative impact of disinformation, rather than just punishing it after the fact.

[336] "Intelligence community" refers to the eighteen different agencies and sub-agencies that report to the Office of the Director of National Intelligence and share a role in collecting, analyzing, evaluating, and disseminating intelligence. For further information regarding the structure and function of the intelligence community, see *Who We Are*, OFFICE OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are [perma.cc/7KAB-G5RR] (last visited Mar. 7, 2024).

[337] *See* H.R. Rep. No. 115-1110, at 49-70 (2018) (discussing how these various agencies reacted to Russian active measures during and after the 2016 election).

[338] U.S. DEP'T OF STATE & U.S. AGENCY FOR INT'L DEV., JOINT STRATEGIC PLAN FY 2022-26 12 (2022), https://www.usaid.gov/sites/default/files/2022-05/Final_State-USAID_FY_2022-2026_Joint_Strategic_Plan_29MAR2022.pdf [perma.cc/B5PP-P54D].

[339] *Election Security: Foreign Influence Operations and Disinformation,* CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/mdm (last visited Mar. 7, 2024).

[340] CYBERSEC. AND INFRASTRUCTURE SEC. AGENCY, MIS- DIS-, AND MALINFORMATION: PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS 1 (2021) https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf [perma.cc/K646-W7MW].

Similarly, the FBI and the intelligence community are both active in the space of detecting and deterring foreign interference and, through their international liaisons, are responsible for sharing law enforcement and intelligence information of transnational concern with foreign governments.[341] Many of the same tactics used against American audiences have been used in the United Kingdom to meddle in the Scottish independence referendum, domestic political matters, and Brexit.[342] They have been employed in Ukraine to attribute fake war crimes to Ukrainian forces since the beginning of hostilities in the Donbas region in 2014.[343] And they have also been used to interfere with French presidential elections.[344] Countries facing these threats should share intelligence and best practices on effective responses, and the national security-related agencies described here are the appropriate entities to facilitate that coordination.

But while these agencies with national security purview are the natural repository for government expertise on countering malign foreign influence, they can make strange bedfellows with policy professionals focused on American elections. For decades, anti-propaganda restrictions under the Smith-Mundt Act prohibited the State Department from providing news programming and content intended for a foreign audience to American audiences.[345]

[341] *Counterintelligence: Combatting Foreign Influence*, FED. BUREAU OF INVESTIGATIONS, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [perma.cc/JT75-KM9U] (last visited Mar. 7, 2024); NAT'L INTEL. COUNCIL, INTELLIGENCE COMMUNITY ASSESSMENT: FOREIGN THREATS TO THE 2020 US FEDERAL ELECTIONS, ICA 2020-00078D (Mar. 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf [perma.cc/3L9W-4C7T]; *What We Do*, OFFICE OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are/organizations/mission-integration/es/what-we-do [perma.cc/M2DE-J3Y9] (last visited Mar. 7, 2024).

[342] Mark Landler & Stephen Castle, *No One Protected British Democracy from Russia, U.K. Report Concludes*, N.Y. TIMES (July 21, 2020), https://www.nytimes.com/2020/07/21/world/europe/uk-russia-report-brexit-interference.html [perma.cc/RC84-3RDK].

[343] Karoun Demijian, *Russian Media Fabricated Story About a Child Getting Killed by Ukrainian Shelling, the BBC Says*, WASH. POST (Apr. 8, 2015, 3:11 PM), https://www.washingtonpost.com/news/worldviews/wp/2015/04/08/russian-media-fabricated-story-about-a-child-getting-killed-by-ukrainian-shelling-the-bbc-says [perma.cc/M7FZ-W8YX]/.

[344] Laura Rosenberger & Jamie Fly, *Lessons from France for Fighting Russian Interference in Democracy*, GERMAN MARSHAL FUND OF THE U.S., https://www.gmfus.org/news/lessons-france-fighting-russian-interference-democracy [perma.cc/F38Z-E8JH].

[345] The Information and Educational Exchange Act of 1948, known as the Smith–Mundt Act, created a de facto ban. *See* 22 U.S.C. § 1461 (1948). A de jure ban was in effect from 1972 to 2013. *See* 22 U.S.C. § 1461 (1972); 22 U.S.C. §§ 1461,

During the Cold War, lawmakers were concerned that the State Department would provide its programming meant for foreign audiences (like the programming on Radio Free Europe and Voice of America) to domestic audiences, acting as a de facto propaganda arm of the executive branch.[346]

While the 2012 Smith-Mundt Modernization Act ended this prohibition,[347] national security-related agencies' involvement in messaging and media operations with domestic audiences remains hugely controversial, demonstrated by the public outcry against the Department of Homeland Security's Disinformation Governance Board (DGB).[348] The creation of the DGB resulted in swift condemnation from the political right, as well as civil libertarians and progressives, for its inept rollout, the complete lack of clarity of its mission and scope, the seemingly partisan sympathies of its appointed leadership, the decision to headquarter it in DHS, and general concerns about any governmental effort to ostensibly determine political "truth."[349] As a consequence, DHS officially disbanded the initiative in August 2022.[350] The poor execution of

1461-1a (2012). *See* Weston R. Sager, Note, *Apple Pie Propaganda? The Smith-Mundt Act Before and After the Repeal of the Domestic Dissemination Ban*, 109 NW. L. REV. 511, 512–528 (providing a legislative history of the Smith-Mundt Act); *see also* John Hudson, *U.S. Repeals Propaganda Ban, Spreads Government-Made News to Americans*, FOREIGN POL'Y (Jul. 14, 2013), https://foreignpolicy.com/2013/07/14/u-s-repeals-propaganda-ban-spreads-government-made-news-to-americans [perma.cc/F5S8-TECU].

[346] *See* Sager, *supra* note 345, at 511, 512.

[347] The Smith-Mundt Modernization Act of 2012 was adopted as part of the 2013 National Defense Authorization Act. *See* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 1078, 126 Stat. 1632, 1957–59 (codified as amended at 22 U.S.C. §§ 1461, 1461-1a (2012)); *see also Legislation: Facts About Smith-Mundt Modernization*, U.S. AGENCY FOR GLOB. MEDIA, https://www.usagm.gov/who-we-are/oversight/legislation/smith-mundt-faqs/ [perma.cc/QHN2-AQRU] (last visited Mar. 7, 2024). Even after the Modernization Act, the U.S. Agency for Global Media's main purpose remains providing programming to foreign audiences. It is simply no longer prohibited to positively respond to requests from domestic audiences to receive that content. *Id.*

[348] Taylor Lorenz, *How the Biden Administration Let Right-Wing Attacks Derail its Disinformation Efforts*, WASH. POST. (May 18, 2022), https://www.washingtonpost.com/technology/2022/05/18/disinformation-board-dhs-nina-jankowicz [perma.cc/B5LS-CTGS].

[349] Amanda Seitz & Nomaan Merchant, *DHS Disinformation Board's Work, Plans Remain A Mystery*, ASSOCIATED PRESS (May 5, 2022), https://apnews.com/article/russia-ukraine-europe-united-states-freedom-of-speech-alejandro-mayorkas-69f658351103d4d049083ad20a713e2a [perma.cc/748Y-Y2NS]; Benjamin Hart, *Poorly Conceived Biden Disinformation Board Put on Pause*, N.Y. MAG. (May 18, 2022), https://nymag.com/intelligencer/2022/05/poorly-conceived-biden-disinformation-board-put-on-pause.html [perma.cc/6P8Z-B3HH].

[350] Press Release, Dep't of Homeland Security, Following HSAC Recommendation, DHS Terminates Disinformation Governance Board (Aug. 24, 2022), https://www.dhs.gov/news/2022/08/24/following-hsac-recommendation-

DGB suggests future governmental efforts to counter disinformation are likely to garner a skeptical, if not hostile, reception, with allegations that these efforts constitute "weaponization" of the government against perceived political foes.

But these missteps cannot end efforts to address the significant threat that disinformation poses to our political process. For years, the State Department's Global Engagement Center (GEC), focused on countering malign foreign disinformation, was not subjected to the same sort of public ire as the DGB. This is most likely because the GEC was the direct product of bipartisan legislation—the 2016 Countering Foreign Propaganda and Disinformation Act—passed in the wake of the 2016 election.[351] The State Department even began to push forward the GEC's mission by preempting known sources of disinformation to blunt their impact.[352]

But recently, Republicans in Congress, as well as at the state level, have joined right-leaning groups to target the GEC as impinging on Americans' First Amendment rights.[353] Congressional disputes over the GEC have imperiled its future funding.[354] Additionally, a pair of rightwing publications have joined Texas Attorney General Ken Paxton in suing the State Department, claiming the GEC supported researchers whose work has harmed the publications' ability to attract advertising revenue by identifying them as purveyors of disinformation.[355] The State Department did fund projects by the Global Disinformation Index ("GDI," a London-based non-profit[356]) to research disinformation outside the United States.[357] But the complaint alleges that a State Department-aligned Twitter (now X) account, promoted content from GDI and another disinformation research entity, NewsGuard, which listed the plaintiffs as unreliable news sites, thus harming

dhs-terminates-disinformation-governance-board [perma.cc/CA5S-UD9R].

[351] Countering Foreign Propaganda and Disinformation Act, 22 U.S.C. § 2656 note.

[352] *See* Steven Lee Meyers, *U.S. Tries New Tack on Russian Disinformation: Pre-Empting It*, N.Y. TIMES (Oct. 26, 2023), https://www.nytimes.com/2023/10/26/technology/russian-disinformation-us-state-department-campaign.html [perma.cc/KGP5-MB9D].

[353] *See* Steven Lee Meyers, *State Dept.'s Fight Against Disinformation Comes Under Attack*, N.Y. TIMES (Dec. 14, 2023), https://www.nytimes.com/2023/12/14/technology/state-department-disinformation-criticism.html [perma.cc/7QC4-LK7Z].

[354] *Id.*

[355] *Id.*; *see also* Complaint, Daily Wire, LLC v. Dept. of State, No. 6:2023-CV-609 (E.D. Tex. Dec. 5, 2023).

[356] *Who We Are,* GLOBAL DISINFORMATION INDEX https://www.disinformationindex.org/about [perma.cc/X8DM-J9CV] (last visited Mar. 3, 2024).

[357] *See* Complaint, Daily Wire, *supra* note 355, at 12.

their business.[358] There are no allegations that the State Department or GEC funded or directed these projects identifying the plaintiffs as unreliable news sources. But the complaint seeks a declaration that the defendants' "funding, development, marketing, and promotion of censorship tools, technologies, and censorship enterprises" violates the plaintiffs' First Amendment rights and requests an injunction against any such future conduct.[359]

It is too early to predict the likelihood of success of this lawsuit, but it should be viewed as part of a concerted strategy to reduce the federal government's ability to combat disinformation insofar as those efforts are seen as having a partisan impact (even if there is no evidence they are tied to partisan goals). Even assuming the Global Engagement Center is not defunded and is permitted to continue its mission of identifying foreign sources of disinformation, it is important that the State Department "stay in its lane" to avoid the appearance of attempting to influence domestic politics and engaging in the sort of domestic propaganda long prohibited to it.[360] To do so, the State Department should defer leadership on this issue to agencies charged with a domestic mission. Interagency working groups designed to coordinate government responses to foreign election interference, for example, could be led by the FEC, operating under an explicit congressional mandate.[361] Should the proposed Digital Consumer Protection Commission Act of 2023 become law, its proposed agency could take the lead on interagency efforts to counter foreign disinformation outside the context of elections.

While only government agencies charged with national security missions have the critical resources, competence, and international relationships necessary to marshal the response to transnational disinformation, these entities must play a subsidiary role in battling foreign malign influence in domestic elections. Their role should be limited to information and intelligence sharing, with a focus on shining a light on foreign propaganda and providing the information necessary both for the private sector to react in real-time to the threat and for agencies like the FEC to properly enforce

[358] *Id.* at 19.

[359] *Id.* at 14.

[360] *See* Sager, *supra* note 345, at 519–25.

[361] The FEC has been the subject of significant criticism for failing to regulate online political advertisements, as well as for its recent deadlock on whether to regulate deepfake campaign ads. *See* Daniela Altimari, *FEC Deadlocks on Whether to Govern Deepfake Campaign Ads*, ROLL CALL (June 22, 2023, 4:18 PM), https://rollcall.com/2023/06/22/fec-deadlocks-on-whether-to-govern-deepfake-campaign-ads [perma.cc/2HGN-SVMM]. For the FEC to effectively address the issues raised in this Article, it would almost certainly require a clear and comprehensive directive from Congress about its responsibilities and authorities in carrying out this mission.

regulations to exclude foreign actors from electoral politics. In addition to mandating that the FEC regulate online advertising, deepfakes, and foreign efforts to engage in political advertising, Congress should consider spelling out the relevant government agencies' roles in countering malign foreign influence in electoral politics in any proposed legislation addressing the issue.

CONCLUSION

Foreign malign influence in democratic elections poses a significant and rapidly evolving threat. Even if state and federal legislators succeed in passing well-crafted, thoughtful legislation in response, and the regulations created by that legislation are upheld as consistent with the First Amendment, this change only shifts the risk. For lasting and effective change, we need a "whole of society" response—incorporating numerous governmental agencies, international partners, state and local governments, and private sector actors—to counter the threat. U.S. regulators should expect foreign adversaries to constantly adapt their tactics to evade our efforts. The country cannot underestimate their interest and willingness to expend resources in undermining our democracy. We must bring to bear resources and efforts commensurate to the challenge.

As this Article has shown, there are robust measures we can take to guard our political sphere from foreign disinformation operations that are consistent with broad protections for political speech under the First Amendment. But Congress must act promptly to implement these efforts, as the challenges posed by disinformation will only become increasingly more complex and difficult to root out.