THE NEW FIGHTING WORDS?: HOW U.S. LAW HAMPERS THE FIGHT AGAINST INFORMATION WARFARE

Jill I. Goldenziel[*]

Manal Cheema[†‡]

ABSTRACT

The United States prides itself on freedom of speech and information. However, foreign adversaries have weaponized these prized freedoms against the United States. The First Amendment, the Privacy Act, and other U.S. laws designed to protect Americans' civil liberties paradoxically constrain the United States' ability to combat information warfare by its enemies. This Article argues that the United States must reform laws and doctrine concerning speech, information, and privacy to protect the democratic process and national security. By exploring the example of the Russian threat to the U.S. electoral process, this Article will illustrate how foreign adversaries wield the United States' own laws against it. It will also explain how justifiable concerns with infringement on civil liberties have hindered the United States' response. The Article concludes with recommendations on how courts, legislatures, and policymakers should balance First Amendment and privacy rights with national security interests to combat information warfare.

TABLE OF CONTENTS

INTRODUCTION 83

I. HOW INFORMATION WARFARE WEAPONIZES THE FIRST AMENDMENT 88

A. The Information Warfare Threat: The 2016 Russian Disinformation Campaign 88

---

* Associate Professor of International Law and International Relations, Marine Corps University-Command and Staff College; Affiliated Scholar, Fox Leadership International, University of Pennsylvania. Thank you to Jack Balkin, Maj Gregg Curley (USMC), Ashley Deeks, CDR Russell Evans, USN, Ret.; Noah Feldman, Craig Hayden, Margaret Hu, Ben Jensen, Michael Pine, Ilya Shapiro, Mark Tushnet, and participants in the Maryland Constitutional Law Discussion Group and the 2019 National Intelligence University Faculty Works-in-Progress Conference. This article also benefitted from participants' comments at a presentation at Marine Corps University's Brute Krulak Center for Innovation and Creativity.

† J.D. Candidate, University of Virginia School of Law, 2020. Thanks to Kendall Burchard, Joseph Digirolamo, and Shaan Shaikh for their thoughtful edits. I am also grateful to my family and many unnamed friends for their support.

‡ Views expressed here are the authors' own and do not reflect those of any arm of the U.S. Government. Errors and omissions are our own.

II. HOW U.S. LAW TIES U.S. HANDS 95
A. The New Private Public Square 96
1. Social Media Is Not the Internet, and Neither Is the Public Square 96
2. The Realities of the Public Square 99
3. Virtual Media is not Traditional Media 102
B. Political Speech and Protections for Falsehoods 107
C. The Incitement Standard is Limited in the Internet Context 109
D. Surveillance, Privacy, and the Chilling Effect 112
1. 2018 Executive Order on Election Interference 112
2. The Privacy Act 113

III. REMEDIES 120
A. Doctrinal Remedies 120
1. Distinguish the Internet and Social Media Contexts 120
2. Distinguish the Electoral Context 121
3. Restrict False Speech Designed to Skew Elections 124
4. Restrict Speech by Foreign Individuals in the Electoral Context 127
5. A Note on Principal, Agent, and Attribution Problems 132
B. Reforming Surveillance Laws 133
1. Lessons from the PATRIOT ACT 133
2. Improving Surveillance Laws and the Privacy Act 135
C. Sanctions 138
D. Fighting Foreign-Sponsored Paid Advertisements 139
E. Fighting Fake News 142
F. Fighting Divisive Propaganda 145
1. Reforming the Foreign Agent Registration Act 145
2. Register and Regulate Bots 147
3. Prosecute Operatives Who Target the Right to Vote 148
4. Employing and Improving Counterspeech 149
a. The Revised Smith-Mundt Act 151
b. Expanding Counterterror Counterspeech 154
G. Regulating Online Platforms and Social Media 155
1. Hurdles to Regulating Online Platforms and Social Media 155
2. Avenues for Regulating Online Platforms and Social Media 157
3. "Voluntary" Actions by Online Platforms 160
4. The Utility of Self-Regulation? 166

CONCLUSION 167

INTRODUCTION

The United States prides itself on freedom of speech and information. However, Russia and other foreign actors have weaponized these freedoms against the United States. Most famously, before the 2016 presidential election, Russia used online sources disguised as news outlets to produce and distribute fake news, targeting voters in swing states.[1] Russia then interfered in the 2018 midterm elections and is attempting to influence the 2020 Presidential election.[2] Iran, North Korea, and China are also engaging in coordinated campaigns aimed at spreading disinformation[3] to alter political discourse.[4] The Islamic State, too, has successfully used social media to shape public opinion and the narrative of its conflict with the United States.[5] According to the U.S. Department of Justice ("DOJ"), foreign-influenced

---

1 Philip M. Napoli, *What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMM. L.J. 55, 76 (2018); Natasha Korecki, *'Sustained and Ongoing' Disinformation Assault Targets Dem Presidential Candidates*, POLITICO (Feb. 20, 2019, 6:05 AM), https://www.politico.com/story/2019/02/20/2020-candidates-social-media-attack-1176018.

2 Josh Gerstein, *U.S. Brings First Charge for Meddling in 2018 Midterm Elections*, POLITICO (Oct. 19, 2018, 2:32 PM), https://www.politico.com/story/2018/10/19/first-criminal-case-filed-over-russian-interference-in-2018-midterms-916787.

3 Disinformation is false information that is deliberately and often covertly spread to influence public opinion whereas misinformation is incorrect or misleading information that is inadvertently sent that influences public opinion.

4 Press Release, Daniel R. Coats, Dir. of Nat'l Intelligence, Office of the Dir. of Nat'l Intelligence, DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (Dec. 21, 2018), https://www.dni.gov/index.php/newsroom/press-releases/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certa in-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election; *see also* PRESIDENT DONALD TRUMP, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 35 (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [hereinafter NSS 2017] (citing China and Russia's use of information against Americans online); Alina Polyakova & Daniel Fried, *Democratic Defense Against Disinformation 2.0*, ATLANTIC COUNCIL, June 2019, at 2 (arguing that exposing disinformation campaigns is not enough to combat them); Emily Birnbaum, *Twitter Releases Archive of Iran, Russia-Linked Misinformation Campaigns*, THE HILL (June 13, 2019, 10:30 AM), https://thehill.com/policy/technology/448341-twitter-releases-archive-of-iran-russia-linked-misinformation-campaigns (reporting Twitter's release of archival tweets relating to Iran and Russia-linked misinformation campaigns); Arya Goel et al., *Managing and Mitigating Foreign Election Interference*, LAWFARE (July 21, 2019, 10:00 AM), https://www.lawfareblog.com/managing-and-mitigating-foreign-election-interference (noting that Russia has targeted 19 different countries and the activities of Iran, China, and Saudi Arabia).

5 William Marcellino et al., *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, RAND CORP., at 15 (2017), https://www.rand.org/pubs/research_reports/RR1742.html.

operations like Russia's include covert actions intended to "sow division in our society, undermine confidence in [ ] democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives."[6] Indeed, Russia's disinformation campaigns spurred a national argument over the legitimacy of the U.S. electoral system and how the United States should respond.[7] The 2017 U.S. National Security Strategy repeatedly notes that the threat of information warfare by Russia and China is likely to continue and that the United States' response has been "tepid and fragmented."[8]

One reason for this weak response is that U.S. laws and jurisprudence protecting free speech and privacy were not designed for the technological realities of today. Much First Amendment doctrine is premised on an idealized public square containing a marketplace of ideas. The Supreme Court has even called the Internet "the modern public square."[9] However, this metaphor is inapt for today's social media environment, where private entities control the conditions in which speech is made and heard.

Moreover, many laws that prevent the U.S. Government from collecting data on U.S. persons' First Amendment activities far predate the Internet.[10] Many of these laws were developed in the 1970s, in the context of fears of U.S. Government overreach during the Cold War. They were intended to legally and morally distinguish U.S. Government actions from the Soviets', who surveilled and propagandized their own people.[11] These laws remain

---

6 U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 1 (2018), https://www.justice.gov/ag/page/file/1076696/download [hereinafter CYBER DIGITAL TASK FORCE REPORT].

7 *Id.*; *see also* NSS 2017, *supra* note 4, at 14, 34 (pointing to America's competitors' use of information to attack American institutions and values).

8 NSS 2017, *supra* note 4, at 35.

9 Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

10 This Article defines a U.S. person as "any United States citizen or alien admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States." 22 U.S.C. § 6010 (2017).

11 For example, the Soviet Union engaged in disinformation campaigns against the United States notably in the 1950s, focusing on the country's systemic racism, and in the 1980s, claiming that AIDS was created by American biological weapons experimentation. *See* Ashley Deeks et al., *Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?*, LAWFARE (Oct. 25, 2017, 7:00 AM), https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts (detailing Soviet use of disinformation campaigns to highlight or exaggerate problems in America); Seth G. Jones, *Russian Meddling in the United States: The Historical Context of the Mueller Report*, CSIS (Mar. 27, 2019),

critical to protect civil liberties and curtail abuses of government power. However, the drafters of those laws could not foresee that, years later, Russia would surveil Americans' Internet data and weaponize it against the United States, while the U.S. Government would be barred from accessing its own people's data to fight back.

An example from 2016 acutely illustrates how U.S. laws constrain the country's ability to combat information warfare. In 2016, the State Department ("DOS") proposed to identify social media influencers who were spreading Kremlin messages and target them with counterarguments.[12] However, the Privacy Act of 1974 restricts data collection related to the ways Americans exercise their First Amendment rights. The proposed program could not guarantee that it would not inadvertently collect American citizens' data, and the DOS program did not fall under the Act's law-enforcement exceptions. State Department lawyers quashed the program, reasoning that tweets, retweets, and comments implicate the collection of data related to the ways Americans exercise their First Amendment rights. The State Department lawyers thus reasoned that the First Amendment prohibited a program that would have encouraged the First Amendment right to free political debate by adding political speech to the marketplace of ideas.[13]

In this and other ways, the United States' own laws tie its hands in its fight against information warfare. For this reason, developing, updating, and deconflicting the laws regulating information operations is a high

---

https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report (arguing that Russia engaged in attempts to influence U.S. elections during the Cold War). Also, during this time period, the U.S. intelligence community frequently violated Americans' civil liberties, which eventually led to the formation of the Church Committee. *See, e.g.*, Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 806–07 (1989) (detailing congressional inquiries into intelligence agencies that uncovered privacy infringements post-Watergate).

12 *See* Adam Entous et al., *Kremlin Trolls Burned Across the Internet as Washington Debated Options*, WASH. POST (Dec. 25, 2017), https://www.washingtonpost.com/world/national-security/kremlin-trolls-burned-across-the-internet-as-washington-debated-options/2017/12/23/e7b9dc92-e403-11e7-ab50-621fe0588340_story.html (detailing the proposed CIA action of creating fake websites and personas to fight back against Kremlin trolls).

13 *Cf.* Jamie Condliffe, *The Week in Tech: Disinformation's Huge Inaction Problem*, N.Y. TIMES (May 31, 2019), https://www.nytimes.com/2019/05/31/technology/facebook-disinformation-nancy-pelosi.html ("[L]awmakers worry about running afoul of the First Amendment . . . .").

government priority.[14] This Article argues that the United States must reform laws, doctrine, and policies to protect national security and the democratic process. First Amendment jurisprudence and the Privacy Act, in particular, pose substantial obstacles to a whole-of-government approach in fighting the Russian disinformation campaign and information warfare more broadly.

Fortunately, solutions to this critical First Amendment problem can be found within First Amendment jurisprudence itself.[15] The First Amendment remains the paramount American constitutional freedom. The Article does not argue that the First Amendment is outdated or should be changed. Instead, the Article argues that the First Amendment must be reinterpreted to continue to protect the values embedded within it. Free and fair elections are the foundation of democratic governance. For this reason, courts give primacy to political speech. Yet, the threat of information warfare now requires reconceptualizing political speech for the Internet era to protect American democracy. Judges, legislators, and policymakers must carefully balance constitutional rights with national security concerns so as not to infringe upon fundamental American freedoms.

The Article proceeds in four parts. Part I will outline how foreign adversaries have waged information warfare against the United States, using the example of Russian information operations targeting the 2016 U.S. presidential election, the most widely-known example of information warfare against the United States.[16] Part II will explain how First Amendment doctrine, the Privacy Act, and related laws constrain the United States' ability to fight information warfare. The Article will argue that Supreme Court doctrine involving the public square, counterspeech, and falsehoods is

---

14 U.S. DEP'T OF DEF., STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT 13 (2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

15 *See* Polyakova & Fried, *supra* note 4, at 3 ("Freedom of expression and US First Amendment protections do not rob free societies of options.").

16 NSS 2017, *supra* note 4, at 14, 34; Press Release, Daniel R. Coats, Dir. of Nat'l Intelligence, Office of the Dir. of Nat'l Intelligence, DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (Dec. 21, 2018), https://www.dni.gov/index.php/newsroom/press-releases/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election.

inadequate for the realities of online political discourse.[17] It will further argue that Cold War-era privacy laws now pose an enormous hurdle to the United States' ability to combat Russia's information warfare. Part IV will outline doctrinal, legislative, and policy solutions to enable the United States to fight information warfare while preserving civil liberties. It will argue that current Supreme Court precedent can be extended to protect the electoral process and regulate foreign speech, and certain other speech, accordingly. The Article will then propose legal reforms, legislation, and new policies to combat three major tactics of election-related Russian information warfare: paid advertisements, fake news, and divisive propaganda. It will also evaluate past proposals for self-regulation by online platforms and social media outlets.[18] Finally, the Article will conclude by discussing the implications of this analysis for the United States' fight against information warfare and the appropriate balance between civil liberties and national security more generally.

This Article will discuss how the United States can combat information warfare through a whole-of-government approach, with a focus on civilian government agencies. A thorough discussion of U.S. military operations concerning information warfare involves additional legal authorities, including classified information, and lies beyond the scope of this paper.[19] However, the framework in this Article is relevant for employing and combatting information operations. Information operations are increasingly used by the U.S. military and its adversaries both during and outside the sphere of armed conflict. U.S. military information operations and surveillance activities—especially when the military operates in cooperation

---

17 This Article considers social media companies as "information content provider[s]" because of their partial responsibility for the "creation or development of information provided through the Internet . . . ." Communications Decency Act of 1996, 47 U.S.C. § 230(f)(3) (2017). The Communications Decency Act was Title V of the Telecommunications Act of 1996, Pub. L. No. 104–104, §§ 501-61, 110 Stat. 56, 133–43 (codified as amended in sections of 47 U.S.C.).

18 Following common practice by courts and legislatures, this Article defines "online platform" as "any public-facing Internet Web site, Web application, or digital application, including a social network or publication, that has 10,000,000 or more unique monthly United States visitors or users for a majority of months during the preceding 12 months." Some courts and statutes have reduced the number of users required to meet this definition. CAL. BUS. & PROF. CODE § 17940(c) (2018).

19 For additional legal authorities relevant to the military's response to information warfare, see generally JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEFENSE, JOINT PUB. 3-12, CYBERSPACE OPERATIONS (June 8, 2018) (providing "joint doctrine to plan, execute, and assess cyberspace operations").

with civilian agencies—must comply with the same constitutional principles discussed in this Article and would employ similar tools to combat misinformation and propaganda campaigns.

I. HOW INFORMATION WARFARE WEAPONIZES THE FIRST AMENDMENT

A. The Information Warfare Threat: The 2016 Russian Disinformation Campaign

Unable to match the United States in conventional warfare, its enemies have turned to stealthier and less costly disinformation campaigns.[20] Russia engaged in a multi-year, coordinated disinformation effort through its state-sponsored Internet Research Agency ("IRA"). The campaign's goal was to exert political influence and exacerbate social divisions within the United States.[21] Russian information warfare adopts a guerrilla or "firehose of

---

20 YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 24 (2018) (defining misinformation as "publishing wrong information without meaning to be wrong or having a political purpose in communicating false information" and disinformation as "manipulating and misleading people intentionally to achieve political ends").

21 NEW KNOWLEDGE, THE TACTICS & TROPES OF THE INTERNET RESEARCH AGENCY 4 (2018), https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf [hereinafter NEW KNOWLEDGE REPORT]; *see also* BENKLER ET AL., *supra* note 20, at 237 (noting the origins of Russian state-sponsored information campaigns against opponents). While this Article cites the New Knowledge Report, it is important to recognize that those concerned about foreign disinformation campaigns are not impervious to conducting their own. The chief executive of New Knowledge, Jonathon Moore, was reportedly involved in a project that engaged in deceptive tactics in the Alabama Senate race between Doug Jones and Roy S. Moore. *See, e.g.*, Scott Shane & Alan Blinder, *Secret Experiment in Alabama Senate Race Imitated Russian Tactics*, N.Y. TIMES (Dec. 19, 2018), https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html. The project involved operators "pos[ing] as conservative Alabamians, using it to try to divide Republicans" and engaging in false-flag operations. Morgan claimed that the project was an "experiment" and not designed "to affect the election." *Id.* Whether or not that is true, it is clear that Americans may seek to engage in disinformation tactics. *See* Emily Birnbaum & Olivia Beavers, *Americans Mimic Russian Disinformation Tactics Ahead of 2020*, HILL (May 8, 2019, 6:00 AM), https://thehill.com/policy/cybersecurity/442620-americans-mimic-russian-disinformation-tactics-ahead-of-2020 (reporting "both right-wing and liberal trolls engage in disinformation campaigns designed to undermine 2020 presidential candidates"); Cat Zakrzewski, *The Technology 202: Disinformation Spread by Americans is 'the Hardest Challenge That We Have,' DHS Official Says*, WASH. POST (Apr. 12, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/04/12/the-technology-202-disinformation-spread-by-americans-is-the-hardest-challenge-that-we-have-dhs-official-says/5caf9cf91ad2e567949ec16c/?noredirect=on&utm_term=.64331b7d0203 (describing disinformation spread by Americans as the hardest challenge government faces).

falsehood" approach,[22] called the Gerasimov Doctrine. The Doctrine proposes that Russia can defeat its enemies through a "combination of political, economic, informational, technological, and ecological campaigns."[23] The Doctrine advocates using non-military tactics over conventional warfare to achieve political and strategic goals.[24] Three distinctive features characterize the model: (1) engaging in a high number of platforms, (2) producing rapid, continuous, repetitive floods of messaging, and (3) disseminating partial truths or outright lies, whether or not they are consistent with one another.[25] Russia's disinformation campaign functions by trying thousands of tactics until one succeeds.

The Gerasimov Doctrine's foundations play on human psychology. First impressions are incredibly resilient: an individual is more likely to accept and favor the first information she receives on a topic when encountering conflicting messages.[26] Research demonstrates that people are likely to remember information, or how they feel about that information, but forget the context in which they learned it.[27] If a user receives misinformation first, she is likely to believe that misinformation, even if she encounters the true information later. Also, receiving a message from multiple media types and multiple sources increases its perceived credibility. This repetitive feature of the Russian "firehose" model breeds familiarity, which leads to acceptance.[28] Termed the illusory truth effect, people "rate statements as more truthful, valid, and believable when they have encountered those statements

---

22 Christopher Paul & Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter It*, RAND CORP. 1 (2016), https://www.rand.org/pubs/perspectives/PE198.html.

23 Peter Pomerantsev, *Inside the Kremlin's Hall of Mirrors*, GUARDIAN (Apr. 9, 2015, 1:00 AM), https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology.

24 Valery Gerasimov, *Contemporary Warfare and Current Issues for the Defense of the Country*, MIL. REV. (Harold Orenstein trans., Nov.–Dec. 2017), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Contemporary-Warfare-and-Current-Issues-for-the-Defense-of-the-Country.pdf.; Ben Sohl, *Influence Campaigns and the Future of International Competition*, REALCLEAR DEFENSE (Sept. 12, 2017), https://www.realcleardefense.com/articles/2017/09/12/influence_campaigns_and_international_competition_112280.html.

25 Paul & Matthews, *supra* note 22, at 1.

26 *Id.* at 4.

27 David M. J. Lazer et al., *The Science of Fake News*, 359 SCIENCE 1094, 1095 (2018), http://science.sciencemag.org/content/sci/359/6380/1094/full/pdf.http://science.sciencemag.org/content/sci/359/6380/1094.full.pdf.

28 Paul & Matthews, *supra* note 22, at 4.

previously than when they are new statements."[29] Thus, many Americans are susceptible to Russian tactics, which exploit psychological tendencies.

The IRA intended to polarize and divide the American electorate and to normalize viewpoints that were strategically advantageous to Russia. The FBI, CIA, and NSA commissioned the Intelligence Community Assessment ("ICA"), a 2017 report to assess Russian activities and intentions in the 2016 election.[30] The report explained that Russian influence campaigns are "multifaceted and designed to be deniable because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations."[31] The influence campaign leading up to the 2016 presidential election blended covert intelligence operations with overt efforts "by Russian Government agencies, state-funded media, [and] third-party intermediaries. . . ."[32] Paid trolls also spread propaganda on social media, and in online chat rooms, discussion forums, and website comment sections.[33] These propagandists maintained thousands of fake accounts on online platforms like Twitter and Facebook.[34] Instagram, in particular, was a target and will continue to be a target as many young social media users use the platform.[35] Instagram's recommendation algorithm, hashtagging, and sharing stories function made it "the most effective platform for the [IRA]."[36]

The Russian effort flooded the Internet, especially social media, with disinformation. According to a report commissioned by the Senate

---

29 *Id.*

30 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ICA 2017-01D, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION, (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf. [hereinafter ICA].

31 *Id.* at 2.

32 *Id.* at ii.

33 *Id.* at 2.

34 Dmitry Volchek & Daisy Sindelar, *One Professional Russian Troll Tells All*, RADIO FREE EUR.: RADIO LIBERTY (Mar. 25, 2015, 11:08 GMT), https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html (discussing a "troll factory" and the assignments given to those who worked there).

35 Taylor Lorenz, *Instagram is the Internet's New Home for Hate*, ATLANTIC (Mar. 21, 2019), https://www.theatlantic.com/technology/archive/2019/03/instagram-is-the-internets-new-home-for-hate/585382/ (noting that users of Instagram, which is "teeming with [ ] conspiracy theories, viral misinformation and extremist memes," are very young); *see also* Paris Martineau, *How Instagram Became the Russian IRA's Go-To Social Network*, WIRED (Dec. 17, 2018, 1:13 PM), https://www.wired.com/story/how-instagram-became-russian-iras-social-network/ (detailing the success of the IRA's efforts on Instagram).

36 NEW KNOWLEDGE REPORT, *supra* note 21, at 26.

Intelligence Committee,[37] the IRA's operations from 2013 to 2018 reached 126 million Facebook users, 20 million Instagram users,[38] and 1.4 million Twitter users. The IRA uploaded one thousand videos on YouTube as well.[39] Between 2015 and 2017, over 30 million users shared Facebook and Instagram posts generated by the IRA.[40]

The Russian disinformation campaign involved at least three major tactics: (1) paid advertisements, (2) fake news, especially false news stories about political candidates, and (3) what we term "divisive propaganda,"[41] which may involve false news stories about other topics or other information operations designed to sow discord in American society. For example, the IRA ran polarizing advertisements on dozens of proxy news sites that disguised or downplayed their affiliation with Russia.[42] IRA accounts were registered at various IP addresses so they could pass for accounts of different nationalities. These advertisements targeted all parts of the political spectrum and reached, at least, hundreds of thousands of Americans.[43] One

---

37 PHILIP N. HOWARD ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT: THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE U.S., 2012-2018, at 6 (2018), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report.pdf [hereinafter OXFORD REPORT].

38 NEW KNOWLEDGE REPORT, *supra* note 21, at 33.

39 *Id.* at 6.

40 OXFORD REPORT, *supra* note 37, at 3; BENKLER ET AL., *supra* note 20, at 242.

41 This Article uses the definition of "propaganda" in the Foreign Agents Registration Act, 22 U.S.C. § 611(j) (1942), *amended by* Lobbying Disclosure Act of 1995, Pub. L. No. 104-65, 109 Stat. 691. The Act defines "political propaganda" to include:

> any oral, visual, graphic, written, pictorial, or other communication or expression by any person (1) which is reasonably adapted to, or which the person disseminating the same believes will, or which he intends to, prevail upon, indoctrinate, convert, induce, or in any other way influence a recipient or any section of the public within the United States with reference to the political or public interests, policies, or relations of a government of a foreign country or a foreign political party or with reference to the foreign policies of the United States or promote in the United States racial, religious, or social dissensions, or (2) which advocates, advises, instigates, or promotes any racial, social, political, or religious disorder, civil riot, or other conflict involving the use of force or violence in any other American republic or the overthrow of any government or political subdivision of any other American republic by any means involving the use of force or violence.

Definitions of propaganda are not consistent in U.S. laws.

42 Paul & Matthews, *supra* note 25, at 2 ("[T]here are dozens of proxy news sites presenting Russian propaganda, but with their affiliation with Russia disguised or downplayed"); *see also* BENKLER ET AL., *supra* note 20, at 368 (discussing Russia's use of behavioral marketing techniques to influence public opinion).

43 Cecilia Kang et al., *Russia-Financed Ad Linked Clinton and Satan*, N.Y. TIMES (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/us/politics/facebook-google-twitter-russian-interference-hearings.html (noting that Facebook had stated that "an estimated 150 million users of its main site and its subsidiary, Instagram, were exposed" to these advertisements).

of the earlier instances of fake news produced by the Russian disinformation campaign was the September 2014 #ColumbianChemicals hoax.[44] The campaign, waged by thousands of Russian troll and bot accounts,[45] centered on an invented explosion at the Columbian Chemicals plant in Louisiana. Related disinformation spread across Twitter, Facebook, and Wikipedia, backed by digitally altered graphics and pictures.[46] Russia also disseminated fake news claiming that Hillary Clinton sold weapons to ISIS.[47]

The majority of the Russian disinformation campaign involved divisive propaganda. These efforts were designed to sow discord in American society, using speech that was sometimes true and sometimes false. For example, IRA efforts on Facebook and Instagram were designed to reinforce themes and messages to clearly-identified audiences, such as the political Left, Right, and African-American communities.[48] Twitter accounts provided "largely opportunistic real-time chatter" and were part of a cross-platform building tactic, linking platform pages with Twitter accounts.[49] Facebook and Instagram were "used to develop deeper relationships" with targeted audiences, building pages "dedicated to continual reinforcement of in-group and out-group ideals."[50] More than one hundred Twitter accounts went as far as to impersonate state and local news enterprises.[51] On Facebook, the five most-shared and the five most-liked posts focused on gun

---

44 Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND CORP. 19 (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf (recounting the Columbian Chemicals plant explosion hoax).

45 This Article defines "bot" as an "automated online account where all or substantially all of the actions or posts of that account are not the result of a person." CAL. BUS. & PROF. CODE § 17940(a) (2018).

46 Helmus et al., *supra* note 44, at 18; *see also* OXFORD REPORT, *supra* note 37, at 26–27 (describing the Columbian Chemical hoax); Adrian Chen, *The Agency*, N.Y. TIMES MAG. (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html (discussing generally the propaganda the IRA posted online under fake identities).

47 *See* ICA, *supra* note 30, at 4 (noting an interview with Julian Assange titled *Clinton and ISIS Funded by the Same Money*); NEW KNOWLEDGE REPORT, *supra* note 21, at 60, 84 (noting that content on right-leaning Internet pages included statements that Hillary Clinton founded ISIS); Max Boot, Opinion, *Without the Russians, Trump Wouldn't Have Won*, WASH. POST (July 24, 2018, 6:36 PM), https://beta.washingtonpost.com/opinions/without-the-russians-trump-wouldnt-have-won/2018/07/24/f4c87894-8f6b-11e8-bcd5-9d911c784c38_story.html.

48 NEW KNOWLEDGE REPORT, *supra* note 21, at 8.

49 *Id.* at 20.

50 *Id.*

51 *Id.* at 66.

ownership, police violence against African-Americans, and anti-immigrant sentiment.[52] Other divisive posts pitted immigrants against veterans and featured messages that were anti-Muslim and anti-President Obama.[53] From 2015 to 2016, much of the divisive messaging sought to benefit then-presidential candidate Donald Trump.[54]

Leading up to the election, the IRA varied its content according to the targeted group. The Agency's messaging was not always "objectively false," and although it may have been offensive, most of it did not qualify as "hate speech."[55] IRA messaging encouraged right-wing groups to support Trump's campaign and to generate anger towards and suspicion of the Left.[56] IRA messaging repeated patriotic and anti-immigrant slogans and attempted to incite outrage about liberal appeasement of 'others' at the expense of U.S. citizens.[57] For example, posted content discussed voter fraud and gave warnings on how the election might be stolen.[58] This messaging directly encouraged votes for Trump.

The IRA acted specifically to suppress votes of those likely to vote against Trump. Left-wing groups and Black Americans, who were expected to vote against Trump, received messaging designed to discourage, confuse, or distract them from voting.[59] The IRA advanced three major variants of voter suppression tactics: "malicious misdirection," designed to create confusion over voter rules; "candidate support redirection," designed to change voting

---

52 OXFORD REPORT, *supra* note 37, at 7.

53 *Id*.

54 ICA, *supra* note 30, at 1 ("We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.").

55 NEW KNOWLEDGE REPORT, *supra* note 21, at 99. Building consensus in the legal community on a definition for hate speech is unavailing. *See generally* Andrew F. Sellars, *Defining Hate Speech* 24–31 (Berkman Klein Center, Working Paper No. 2016-20, 2016) (attempting to define hate speech by drawing out eight common traits of hate speech definitions).

56 NEW KNOWLEDGE REPORT, *supra* note 21, at 83; *see also* BENKLER ET AL., *supra* note 20, at 236 ("Just as terrorism succeeds most when it evokes an overreaction and causes a society to respond from fear and anger rather than calculation, so too will Russian active measures have their largest effect through evoking a harmful autoimmune response from the countries under attack."). The "Left" here is used colloquially to refer to liberals and Democrats, as opposed to moderates, conservatives, or Republicans.

57 OXFORD REPORT, *supra* note 37, at 19.

58 NEW KNOWLEDGE REPORT, *supra* note 21, at 81 (describing voter suppression tactics employed by the IRA in the days leading up to the election).

59 OXFORD REPORT, *supra* note 37, at 19; BENKLER ET AL., *supra* note 20, at 240 ("The core strategy . . . was to increase disaffection, distrust, and polarization in American politics.").

patterns; and "turnout depression."[60] To illustrate, the IRA advanced the message that voters should boycott the election because the candidates do not care about Black people.[61] The messaging preyed on societal anger with structural inequalities, police violence, and disproportionate levels of incarceration.[62] When it came to messaging directed at the Left, the IRA sought to promote anti-establishment views and redirect candidate support[63] by using messaging designed to reduce trust in the political system.[64] IRA content also adopted specific political stances, mentioning Trump and Clinton by name.[65] The ICA concluded—with high confidence—that Russia's goals were to undermine the U.S. democratic process and harm Hillary Clinton's electability and potential presidency.[66]

The IRA's campaigns did not stop with the 2016 election or even when the U.S. intelligence community caught them. To the contrary, engagement rates increased and covered a broader range of public policy and national security issues, along with social issues relevant to younger voters.[67] The ICA warned that Russia and other foreign adversaries are likely to expand on these tactics to meddle in future elections and further polarize American society.[68] FBI Director Chris Wray declared in July 2018 that "malign influence operations" by Russia and others are actively underway.[69] Russia's defense minister has also announced plans to expand its information warfare capability.[70]

---

60 NEW KNOWLEDGE REPORT, *supra* note 21, at 8.

61 OXFORD REPORT, *supra* note 37, at 3.

62 *Id*. at 19.

63 NEW KNOWLEDGE REPORT, *supra* note 21, at 83 (noting that left-targeted content focused on identity and pride, and encouraged voting for candidates other than Clinton).

64 OXFORD REPORT, *supra* note 37, at 20 (describing messaging to LGBT and liberal voters as seeking to reduce trust in the political system).

65 NEW KNOWLEDGE REPORT, *supra* note 21, at 76 (stating that approximately 6% of tweets, 18% of Instagram posts, and 7% of Facebook posts mentioned the candidates by name).

66 ICA, *supra* note 30, at 1.

67 OXFORD REPORT, *supra* note 37, at 3.

68 Joseph Thai, *The Right to Receive Foreign Speech*, 71 OKLA. L. REV. 269, 273–74 (2018) (citing ICA, *supra* note 30, at 5).

69 Connor O'Brien, *FBI Director: Russia 'Continues to Engage in Malign Influence Operations' Against U.S.*, POLITICO (July 18, 2018, 9:50 PM), https://www.politico.com/story/2018/07/18/fbi-wray-russia-meddling-732337.

70 *See* Vladimir Isachenkov, *Russia Military Acknowledges New Branch: Info Warfare Troops*, AP NEWS (Feb. 22, 2017), https://apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c/russian-military-continues-massive-upgrade (discussing "information warfare troops," Russia's new branch of the military).

Congress directed the Secretary of Defense to assess his department's capability to engage with social media and publicly available information in May 2016, which was too late to stop Russian interference in the presidential election.[71] The precise impact of these disinformation campaigns on elections is hard to measure, which may have made some government actors reluctant to devote resources to stop them. However, the campaigns have undoubtedly succeeded in sowing dissension in American society, creating protests over fake issues online.[72] Regardless of whether they changed the outcome of any given election, the United States must stop its adversaries from weaponizing American freedoms to cause dissension and violence within its borders.

Any legislation or regulatory oversight relating to social media will clash with U.S. doctrine on free speech. The United States' commitment to free speech and privacy creates an asymmetric disadvantage against Russia and other adversaries who routinely engage in censorship, manipulation, and suppression of ideas.[73] The New Knowledge Report highlights that "[o]ur deeply-felt national scruples about misidentifying a fake account or inadvertently silencing someone, however briefly, create a welcoming environment for malign groups who masquerade as Americans or who game algorithms."[74] To combat Russian threats to the U.S. democratic process—and to social order more generally—the United States must confront how its domestic law constrains its ability to fight information warfare. Stronger rules and norms are also needed to prevent the use of social media and new information technologies to manipulate U.S. elections.[75]

II. HOW U.S. LAW TIES U.S. HANDS

First Amendment freedoms create an environment ripe for Russia's disinformation campaigns. As Eric Posner explains, the "First Amendment

---

71 H.R. REP. NO. 114-537, at 91, 246–47 (2016) (acknowledging that the Department of Defense lacked sufficient capacity and directive to address information warfare and directing the Department to assess and address the issue).

72 *See e.g.*, Claire Allbright, *A Russian Facebook Page Organized A Protest in Texas. A Different Russian Page Launched the Counterprotest.*, TEX. TRIB. (Nov. 1, 2017, 4:00 PM), https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l/.

73 *Id.*

74 NEW KNOWLEDGE REPORT, *supra* note 21, at 100.

75 *Id.* (noting that more investigation needs to be done to understand and address information warfare threats to U.S. elections).

protects propagandists whom U.S. authorities could reach, and national borders protect propagandists whom the First Amendment does not protect."[76] In short, the First Amendment gives the highest protection to political speech, which, under Supreme Court precedent, applies to many Russian disinformation efforts. The First Amendment also protects falsehoods, and caselaw suggests this would include much Russian fake news.[77] Counterspeech, the presumptive remedy to false speech, is limited in its utility. The Supreme Court's doctrine on incitement, one of the few areas of speech that is not protected by the First Amendment, likely does not extend to Russian disinformation campaigns in its current form. Concerns with surveillance infringing on privacy and chilling speech also inhibit the U.S. Government's ability to respond to Russian disinformation campaigns. Any legislation that would allow the United States to combat information warfare must overcome these hurdles.

A. The New Private Public Square

Many of the Supreme Court's seminal cases on freedoms of speech and the press were decided before the advent of the Internet, social media, and big data. Therefore, the factual assumptions of those cases do not transplant perfectly onto today's social media environment. When the Internet made it far easier to extend the reach of disinformation beyond a country's borders, it fundamentally altered the scope of the First Amendment. The law remains stagnant. The Supreme Court has tried to graft the metaphor of the public square, the paradigmatic venue for the exchange of free speech and ideas, onto the Internet context. However, the Supreme Court's analysis suffers from several critical flaws, including the failure to distinguish social media from the Internet at large, the failure to distinguish social media from traditional media, and the limits of counterspeech.

1. Social Media Is Not the Internet, and Neither Is the Public Square

Supreme Court jurisprudence lumps the Internet together with social media as part of the "new public square." The first Internet-related case resolved in the Supreme Court was *Reno v. American Civil Liberties Union*, in

---

76 Eric Posner, *Are Russian Trolls Protected by the First Amendment?*, ERIC POSNER (Feb. 17, 2018), http://ericposner.com/are-russian-trolls-protected-by-the-first-amendment/.

77 *See, e.g.*, United States v. Alvarez, 567 U.S. 709 (2012).

which the Court established that online speech does not receive a lesser degree of First Amendment protection than other speech.[78] In *Reno*, the ACLU sued the U.S. Attorney General, claiming that two provisions of the Communications Decency Act of 1996 ("CDA") violated the First Amendment.[79] The provisions criminalized the "knowing transmission of obscene or indecent" messages to minors, and "knowing, sending, or displaying of patently offensive messages" to minors that contain "sexual or excretory activities or organs."[80] The Supreme Court held that "the blanket provisions were an impermissible infringement on free speech rights."[81] The provisions "were content-based restrictions because they regulated the subject matter and type of speech," and therefore were subject to strict scrutiny.[82] The Court found the content-based restrictions to be overbroad and vague, as "indecent" and "obscene" were not defined.[83] Although *Reno* did not specifically involve social media websites, courts later relied on this case when extending First Amendment protection to social media.

In the early 2010s, district courts extended *Reno* to find that the First Amendment protects a wall post[84] and "liking" a political candidate's

78 521 U.S. 844, 870 (1997) ("[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]."); *see also* Ostergren v. Cuccinelli, 615 F.3d 263, 272 (4th Cir. 2010) (recognizing the Internet standard presented in *Reno*).

79 *Reno*, 521 U.S. at 861.

80 *Id*. at 859–60. The first provision, 47 U.S.C. § 223(a), "prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age." *Id.* at 859. The second provision, 47 U.S.C. § 223(d), "prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age." *Id.*

81 Katherine A. Ferry, Comment, *Reviewing the Impact of the Supreme Court's Interpretation of "Social Media" As Applied to Off-Campus Student Speech,* 49 LOY. U. CHI. L.J. 717, 743 (2018); *see also Reno*, 521 U.S. at 868 (noting that the CDA is a "content-based blanket restriction on speech"); Andrew H. Montroll, Note, *Students' Free Speech Rights in Public Schools: Content-Based Versus Public Forum Restrictions*, 13 VT. L. REV. 493, 500 (1989) (describing the Supreme Court's traditionally strict approach to content-based speech restrictions).

82 *See* Blum et al., *Tests to be Applied to Content-Based and Content-Neutral Regulations*, 16A AM. JUR. 2D *Constitutional Law* § 480 (2017) (describing the analysis concerning content-based restrictions).

83 *Reno*, 521 U.S. at 877–79.

84 *See* Mattingly v. Milligan, No. 4:11CV00215(JLH), 2011 WL 5184283 (E.D. Ark. Nov. 1, 2011) (holding that a public employee's Facebook post was protected under the First Amendment); Gresham v. City of Atlanta, No. 1:10-CV-1301-RWS, 2011 WL 4601020 (N.D. Ga. Sept. 30, 2011) *adhered to on reconsideration*, No. 1:10-CV-1301-RWS, 2012 WL 1600439 (N.D. Ga. May 7, 2012) *and aff'd*, 542 F. App'x 817 (11th Cir. 2013) (concluding that the plaintiff's Facebook post was entitled to First Amendment protection).

Facebook page.[85] In the 2017 case of *Packingham v. North Carolina*, the first Supreme Court case to address social media, the Court struck down a North Carolina statute that prohibited sex offenders from accessing social media sites.[86] Justice Kennedy, writing for the majority, famously characterized the Internet as "the new public square."[87] Kennedy noted that 70% of American adults were then using at least one social media site, and Facebook's membership—the particular site at issue—was three times the size of North America's population.[88] While the Court likened the Internet to the public square, the worldwide reach of the Internet has outgrown any physical public square in its role as a channel for expression.[89] The Court explained that social media websites:

> can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard. They allow a person with an Internet connection to 'become a town crier with a voice that resonates farther than it could from any soapbox.' In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights.[90]

This reasoning underscores the role of social media as a public forum for speech.

The Court recognized that legislatures could limit First Amendment protection for sex offenders using narrowly tailored statutes. However, it found that the statute at issue, though content-neutral, burdened more speech than was necessary to advance the government's interest in protecting vulnerable victims from dangerous predators.[91] Thus, North Carolina did not meet its burden of showing that a sweeping law barring access to social media sites is necessary or legitimate to serve the stated purpose of keeping sex offenders away from vulnerable victims.

---

85 Bland v. Roberts, 730 F.3d 368, 386, 394 (4th Cir. 2013) (finding that "liking" a Facebook page is speech protected by the First Amendment but remanding on other grounds).

86 137 S. Ct. 1730 (2017).

87 *Id*. at 1737 (describing the Internet as "the modern public square").

88 *Id*. at 1735; *see also* Facebook, *Company Info*, FACEBOOK NEWSROOM, https://newsroom.fb.com/company-info/ (last visited Oct. 20, 2019) (noting that there were "1.59 billion daily active users on Facebook on average for June 2019"); Jessica Guynn, *Facebook Now Averages 8 Billion Daily Video Views*, USA TODAY (Nov. 4, 2015, 8:10 PM), http://usat.ly/2huc6St ("Facebook says it now averages 8 billion daily views from 500 million users.").

89 *Packingham*, 137 S. Ct. at 1737 (referring to the Internet as the "modern public square").

90 *Id*. at 1737 (citing *Reno v. ACLU*, 521 U.S. 844, 870 (1997)).

91 *Id.* at 1737–38.

Packingham thus clarifies that the same First Amendment standards that protect the actual public square also protect social media sites. As discussed below, political speech has traditionally received the highest constitutional protections within the public square. Presuming that foreign propaganda qualifies as protected political speech, foreign disinformation campaigns may then receive the highest level of First Amendment protections.

2. The Realities of the Public Square

The realities of the old public square, however, are quite different from those of the "new" one. The Internet may be a public zone of sorts because of the ability of any user to post and receive information on publicly available sites. Nevertheless, social media serves as the battleground for information campaigns precisely because of attributes that distinguish it from the idealized public square of pre-Internet First Amendment jurisprudence. Moreover, courts have treated "the Internet" as a monolith in their decisions, lumping social media sites together with search engines and Internet retailers. In the context of free speech and political debate, different types of Internet sites present distinct constitutional issues that are critical for combatting information warfare.[92]

Two common types of Internet sites—search engines and social media—present different legal issues related to the First Amendment and privacy. The way users interface with the Google search engine is entirely different from the way users interact with one another on social media. Users of a search engine are presented with the product of search results. A search engine company's responsibility to its users is to provide the most relevant results, and to distinguish for its users those companies who have paid for their results to be advertised. The data that users enter into a search engine is information for which they wish to search, not necessarily personal data about themselves, their family, or their relationships.[93] Social media sites, by contrast, require more personal user interaction. Users enter personal information on a profile and connect with friends or other contacts. They communicate with each other through the site, post and share information, and comment on that information. Most social media sites do not generate

92 The authors acknowledge that, in some contexts, it may be appropriate for the Court to treat social media and other Internet sites similarly. However, we argue that social media presents some unique constitutional issues in the context of political speech and information warfare.

93 We recognize, however, that questions or topics searched can certainly be revealing of one's personal circumstances and other information.

news items on their own, but they allow users to create and share content using the websites as platforms. Social media companies may agree to keep users' data private or publicly available on the Internet. These companies profit from advertisers who target potential customers with user data. Unlike search engines, social media companies do not only provide information; they provide users an experience and advertisers a platform to sell their products.

Perhaps most importantly, private companies govern social media. U.S. persons do not have the same negative rights against private companies as they do against the government. Private companies exist for profit and have the right to accept money for advertising and post-boosting by paid companies without restrictions. Social media companies do exercise a type of governance over the online communities that they have created.[94] Although not all social media sites have as intricate a communal structure as Facebook, they all have terms of service that amount to contracts of adhesion between the companies and their users. However, social media users do not benefit from constitutional protections against their social media "government." Social media companies may engage in data mining that would likely constitute search, seizure, or surveillance and face regulation if done by the U.S. Government.

While social media sites are important venues for discourse and expression, social media differs drastically from the public square. Public squares are sites for human interaction. Visitors to a public square can see who enters and exits, and be sure that they are real people. Visitors can more easily filter out real news sources from fake news sources when interacting with real people. They can see the human source of the news, can directly and instantaneously ask questions about the legitimacy of the source and content, and can better determine the veracity of the information given to them. There is a limit to the amount of information that a person can receive in a public square in a short period. Public squares do not usually have echo chambers that facilitate the repetition of false messages. The capacity to enter a public square and speak in it rarely depends upon whether a State sponsors a speaker or whether one speaker can pay to promote posts more

94 *See generally* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018) (describing the social media platform's regulation of speech as "governance").

than others. Speech is not spoken or heard on social media the way it is in a public square, since a post may be seen and shared long after it is originally "spoken."[95]

Social media is particularly vulnerable to influence and disinformation campaigns in ways that the public square is not. Social media was designed to open unfiltered, personalized channels of communication. It does not possess the filters and vetting systems of traditional news media to process what is true and what is false.[96] Thus, the platforms enable false information to spread widely and quickly.[97] Social networks amplify the reach and effectiveness of sensational stories, including those from foreign speakers acting to influence U.S. political conversations. Precise, targeted advertising capabilities magnify the effect of those wishing to spread disinformation on social media.[98] In 2016, divisive propaganda campaigns delivering targeted messaging to Right, Left, and African-American communities were made more effective by the echo chambers inherent in social media. Further, sharing functions and the wide breadth of the campaign improved the reach of disinformation to members of the targeted communities.

Thus, social media is not a public square and should not be legally treated as such. As Justice Kennedy recognized in *Packingham*, the Internet has increased the size of the public square far beyond what the builders of any physical public square ever conceived. Yet the Supreme Court has failed to recognize the implications of that infinite expansion for the usefulness of this hallowed metaphor. Social media is only one part of the Internet, and both social media and the Internet are distinct from the idealized public square assumed in free speech jurisprudence. Distinguishing between the roles that the Internet and social media play as fora for political speech is critical to creating distinctly tailored constitutional laws and regulations to protect the

---

95 John P. Cronan, *The Next Challenge for the First Amendment: The Framework for an Internet Incitement Standard*, 51 CATH. U. L. REV. 425, 428 (2002) (noting that "the vast majority of Internet communications . . . are usually 'heard' well after they are 'spoken'"). As of November 2019, Cronan is the Principal Deputy Assistant Attorney General for the DOJ Criminal Division.

96 *See* Samantha Power, Opinion, *Samantha Power: Why Foreign Propaganda Is More Dangerous Now*, N.Y. TIMES, Sept. 19, 2017, https://www.nytimes.com/2017/09/19/opinion/samantha-power-propaganda-fake-news.html (discussing the risk of foreign influence online).

97 *See* David M. Howard, *Can Democracy Withstand the Cyber Age: 1984 in the 21st Century*, 69 HASTINGS L.J. 1355, 1371 (2018) (noting the prevalence of disinformation in the media and its impact on the role social media plays).

98 *See* Thai, *supra* note 68, at 307 ("[T]he voluntary clustering of politically likeminded individuals and the application of sophisticated ad targeting, can greatly amplify the reach . . . of a sensational story from a foreign speaker seeking to influence the domestic political marketplace.").

integrity of the electoral process. The metaphor of the "public square" may have been more apt for the Internet early in its history. Today, social media places political discourse under private control and creates an environment ripe for exploitation.

3. Virtual Media is not Traditional Media

Scholars and courts frequently apply a First Amendment framework based on traditional media to the Internet and social media. However, important distinctions might justify different treatment under First Amendment doctrine. As discussed above, social media and the Internet are susceptible to disinformation campaigns in ways that traditional media are not.

Scholar Alan Chen has identified three distinctive features of the Internet compared to other media: broad and instantaneous amplification of information, relatively inexpensive cost, and elements of anonymity.[99] When extending existing First Amendment doctrine to social media, courts might wish to distinguish it on these grounds. The fact that the Internet is faster and cheaper at disseminating information is less likely to be a distinguishing factor; telecommunications have only gotten faster and less expensive over time, with little change to First Amendment jurisprudence as a result. The features of anonymity that the Internet provides drastically change the speaker-audience relationship envisioned in prior First Amendment jurisprudence such that this criterion might be fertile ground for distinguishing the Internet. The ability of a speaker to remain anonymous complicates the question of attribution for speech. Previously, the audience who heard someone shouting "fire" in a crowded theater could look at the speaker and make some judgment as to her credibility to sound such an alarm. On the Internet, a decent graphic designer or video editor can provide a veneer of credibility that would be more difficult for humans to match than in person. Traditional media also involves an important layer of professional editorial review for content that is mostly absent on social media. To the extent that social media companies approve advertisements, they are

99 Alan K. Chen, *Free Speech and the Confluence of National Security and Internet Exceptionalism*, 86 FORDHAM L. REV. 379, 391 (2017).

not subject to the same degree of regulation as law requires for advertisements on broadcast media.[100]

Unlike previous content distributors (e.g., book distributors) and traditional media, social media platforms do little, if anything, to curate the sources and content disseminated on their platforms.[101] Professional rules of conduct and ethical norms bind traditional news outlets and journalists on media platforms. These traditional outlets involve a layer of editorial oversight, often including fact-checking, before publishing a story. Social media contains no such checks for professionalism, ethics, or veracity. The social media user alone bears the burden to distinguish between fake and legitimate news.[102] As discussed below, most consumers are not able to distinguish the sources and determine the legitimacy of the news.

In some circumstances, the lines between online media and regular media blur. Traditional media sites like the *New York Times*, for example, also have websites and interactive functions, and traditional First Amendment interpretations may still be adequate for these sites. However, in the context of information warfare, the failure of courts and commentators to recognize distinctions between online and traditional media is problematic. In this context, traditional media and online media function differently, and social media functions differently from much other Internet media—and vastly different from the public square. Any effective laws to fight information warfare must account for these important distinctions. Even more importantly, courts must interpret such laws based on appropriate, empirically-based assumptions.

4. The Limits of Counterspeech

Much of U.S. First Amendment jurisprudence is based on the doctrine of counterspeech. The counterspeech doctrine proposes that more true

---

100 For example, Federal Election Commission rules regarding advertising and disclosure that apply to traditional media do not apply to social media. *See, e.g.*, *Advertising and Disclaimers*, FED. ELECTION COMMISSION, https://www.fec.gov/help-candidates-and-committees/making-disbursements/advertising/ (last visited Nov. 20, 2019). The Honest Ads Act aimed to close some of these loopholes but was not passed by Congress. *See* Honest Ads Act, S. 1989, 115th Cong. (1st Sess. 2017).

101 Napoli, *supra* note 1, at 85.

102 *See id.* (noting that the "relatively limited ability" of social media platforms "to distinguish between fake and legitimate news stories/sources" has been transferred to the media consumer).

speech will drown out false speech in the Millian marketplace of ideas: a free and competitive speech environment with limited government interference.[103] The doctrine was most famously articulated in Supreme Court jurisprudence by Justice Brandeis in *Whitney v. California* in 1927.[104] In concurrence, Brandeis wrote, "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."[105] For Brandeis, the solution to false speech is to counter it with more speech. True and false speech will compete in the marketplace of ideas until the truth prevails.[106]

Accordingly, counterspeech is often proposed as a solution to respond to falsity in political campaign communications.[107] Yet the counterspeech doctrine rests on several major assumptions that may not be true in any context and are especially mistaken in the social media context. First, it assumes that individuals can distinguish between true and false information.[108] Second, it assumes participants value true information more than false information.[109] Scientific studies cast doubt on both of these assumptions.[110] These studies show that people usually accept information uncritically. They do not usually question the information's credibility unless it challenges their existing assumptions, or they have incentives to do so.

---

103 *See* Daniel E. Ho & Frederick Schauer, *Testing the Marketplace of Ideas*, 90 N.Y.U. L. REV. 1160, 1167 (2015) (observing that Brandeis' concurring opinion in *Whitney v. California* is a "canonical formulation" of the "marketplace of ideas" metaphor); *see also* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[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, and that truth is the only ground upon which their wishes safely can be carried out. That, at any rate, is the theory of our Constitution.").

104 Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

105 *Id*.

106 *See* Alexandra Andorfer, Note, *Spreading like Wildfire: Solutions for Abating the Fake News Problem on Social Media via Technology Controls and Government Regulation*, 69 HASTINGS L.J. 1409, 1422 (2018) (noting Justice Holmes's idea that "true speech should compete with falsehoods in the 'marketplace of ideas' until the truth eventually wins").

107 *See* Rickert v. Pub. Disclosure Comm'n, 168 P.3d 826, 832 (Wash. 2007) ("[T]he best remedy for false or unpleasant speech is more speech, not less speech.").

108 *See* Lyrissa Barnett Lidsky, *Nobody's Fools: The Rational Audience as First Amendment Ideal*, 2010 U. ILL. L. REV. 799, 801 (2010) (noting that counterspeech assumes that audiences can "rationally assess[] the truth, quality, and credibility" of speech).

109 Napoli, *supra* note 1, at 61 (citation omitted).

110 *See* BENKLER ET AL., *supra* note 20, at 5–6 ("This flurry of [research] exhibited a broad sense that as a public we have lost our capacity to agree on shared modes of validation as to what is going on and what is just plain whacky."); Lazer et al., *supra* note 27, at 1095 (discussing studies that show people are "more likely to accept familiar information as true").

Individuals are often inclined to align their beliefs with those in their communities, making echo chambers more powerful.[111] According to a team of law professors and social scientists examining fake news, "[r]esearch also further demonstrates that people prefer information that confirms their preexisting attitudes (selective exposure), view information consistent with their preexisting beliefs as more persuasive than dissonant information (confirmation bias), and are inclined to accept information that pleases them (desirability bias)."[112] Other scholars argue that retractions and refutations are rarely effective, especially as time passes.[113] People may be inclined to accept false information over accurate facts, especially if disinformation is repeated.[114] Thus, social media users may not be able to distinguish true from false information. More surprisingly, depending on their preferences, they may not want to do so.

Third, the doctrine assumes that the speech environment will allow users to distinguish between true and false information.[115] This assumption is especially troubling in the social media environment. False statements like propaganda affect consumers' ability to distinguish real from fake news because false statements disguise the source. Propaganda operations may be anonymous or may masquerade as legitimate news outlets.[116] Adding to the confusion over the veracity of information, legitimate and illegitimate news outlets often exist in the same social media feeds.[117] As Professor Lyrissa Lidsky notes, the concept of a rational audience that can process the news and assess the credibility and truth is a hallowed idea in First Amendment theory but not an empirical reality.[118]

Given what we now know about human psychology, counterspeech may not be sufficient to overcome false news. It might even be counterproductive in some circumstances. Repeating false information, even in the context of

---

111 Lazer et al., *supra* note 27, at 1095.

112 *Id.*

113 Paul & Matthews, *supra* note 22, at 9.

114 Abby K. Wood & Ann M. Ravel, *Fool Me Once: Regulating "Fake News" and Other Online Advertising*, 91 S. CAL. L. REV. 1223, 1269 (2018).

115 Napoli, *supra* note 1, at 61.

116 *Id.* at 83.

117 *Id.*

118 *See* Lyrissa Barnett Lidsky, *Incendiary Speech and Social Media*, 44 TEX. TECH L. REV. 147, 155 (2011) ("First Amendment doctrines dealing with incendiary speech rest largely on the assumption that audiences will behave rationally and not leap to violence when confronted with offensive or inflammatory speech.").

counterspeech, may perversely increase the likelihood that people will believe it. Empirical testing of claim repetition in fact-checking has been inconclusive thus far.[119]

The fourth potentially flawed assumption of the Supreme Court's counterspeech doctrine is that there is no such thing as too much speech. Neither Mill nor Brandeis could have foreseen the overwhelming amount of speech freely available on the Internet and in today's marketplace of ideas.[120] Structural and economic changes in this era of news media and information undermine the view that truth will prevail over falsity.[121] The hyper-sensationalistic attributes, wide dissemination, and ease of production of fake news could theoretically shrink the market for real journalism.[122] The high-volume approach of Russian information warfare can drown out competing messages. Justice Brandeis's formulation of counterspeech assumes sufficient time is available to separate truth from falsehood. In the face of overwhelming amounts of both, separation may not be possible.

Fifth, the doctrine assumes that people exposed to false information are more likely than not to be exposed to corresponding true information.[123] The doctrine did not foresee the social media bubbles that most users inhabit. Counterspeech may never reach those most affected due to highly polarized social media echo chambers.[124] The flawed assumptions underlying the doctrine of counterspeech sharply limit its effectiveness in the social media environment.

Thus, past Supreme Court doctrine on the public square and counterspeech may be incompatible with the context of the Internet and social media. More research is required to discover the conditions under

---

119 Lazer et al., *supra* note 27, at 1095.

120 *See* Frederick Schauer, *Free Speech, the Search for Truth and the Problem of Collective Knowledge*, 70 SMU L. REV. 231, 250 (2017) ("[T]he entire analysis here takes place entirely within a set of search for truth/marketplace of ideas justifications for freedom of speech, a set of justifications that has not fared well when subject to close analytical and empirical scrutiny . . . ."). *See generally* Napoli, *supra* note 1, at 61 (citing McConnell v. FEC, 540 U.S. 93, 259 (2003) (Scalia, J., concurring in part and dissenting in part) ("[G]iven the premises of democracy, there is no such thing as too much speech.").

121 Napoli, *supra* note 1, at 59.

122 Andorfer, *supra* note 106, at 1423–24.

123 *See* Vincent Blasi, *Reading Holmes through the Lens of Schauer: The* Abrams *Dissent*, 72 NOTRE DAME L. REV. 1343, 1357 (1997) ("[T]he efficacy of refutation still turns on whether the counter-message comes to the attention of all persons who were swayed by the original idea.").

124 Thai, *supra* note 68, at 310.

which certain counterspeech methods might work. Counterspeech remains the preferred remedy to false speech and disinformation under current First Amendment doctrine. However, its effectiveness as a remedy in the social media context is doubtful.

B. Political Speech and Protections for Falsehoods

Compounding the challenges of information warfare is that the First Amendment protects "deliberate, nonlibelous falsehoods."[125] In recent years, the Supreme Court has expanded and clarified these protections. In the 2012 case of *United States v. Alvarez*, the Court struck down the Stolen Valor Act, a federal statute that criminalized false claims that one had received military medals.[126] Justice Kennedy, writing for a plurality, asserted that First Amendment cases require the strictest scrutiny, regardless of whether the content of speech is true or false. Few categories of speech, such as obscenity, incitement to imminent lawless action, defamation, fighting words, speech integral to criminal conduct, true threats, and child pornography, are exempt from this ban on content-based regulation. Even then, false speech may be constitutionally protected, as in defamation cases. Under *Alvarez*, false statements can only be regulated if the speaker intended to cause "legally cognizable harm" and a direct causal link exists between the "restriction imposed and the injury to be prevented."[127] Justice Breyer, joined by Justice Kagan in concurrence, said that prohibitions of false speech should receive only intermediate scrutiny. Despite the split holding, *Alvarez* represents the Court's most robust protections for false speech.

Following *Alvarez*, in 2016, the Sixth Circuit struck down a statute that criminalized false statements made about political candidates as unconstitutional suppression of speech and noted potential corresponding chilling effects.[128] Likewise, in 2010, the Ninth Circuit held that "[t]he right to speak and write whatever one chooses—including, to some degree, worthless, offensive, and demonstrable untruths—without cowering in fear of a powerful government is, in our view, an essential component of the protection afforded by the First Amendment."[129] This line of precedent

125 Andorfer, *supra* note 106, at 1428 (citing United States v. Alvarez, 567 U.S. 709 (2012)).

126 United States v. Alvarez, 567 U.S. 709, 730 (2012).

127 *Id.* at 719, 725.

128 Susan B. Anthony List v. Driehaus, 814 F.3d 466, 476 (6th Cir. 2016).

129 United States v. Alvarez, 617 F.3d 1198, 1206 (9th Cir. 2010), *aff'd*, 567 U.S. 709 (2012).

would support the protection of fake news in the electoral context, especially given potential chilling effects.

Supreme Court jurisprudence would not likely support legislation that blocked false or misleading foreign speech merely on social value grounds. For example, in *Brown v. Entertainment Merchants Association*, the Court struck down a state ban on the sale of violent video games to minors because speech, regardless of cultural or intellectual worth, is protected by First Amendment standards.[130] And, in *United States v. Stevens*, the Court invalidated a federal ban targeting fetishistic depictions of animal cruelty because "an ad hoc balancing of relative social costs and benefits" encouraging government regulation infringes on First Amendment values.[131]

Stevens, in particular, suggests that the Court must conclude that the government cannot regulate speech on the basis that it is distasteful or has little social value. Instead, the speech must generate enough adverse effects to justify a censoring of speech. If the government sought to bar speech merely because it had less social value, it would limit the marketplace of ideas. Even if speech has little social value, the First Amendment demands that people can express and communicate their opinions to others, however mistaken, disagreeable, or offensive others may find them. Given this demand, it is unlikely that the government could block false or misleading foreign speech merely on social value grounds.

Thus, under First Amendment jurisprudence, government restrictions on foreign speech, even speech that promotes falsehoods, are likely unconstitutional.[132] A plurality of the Court has held that the First Amendment protects fake news and that the government cannot restrict speech of questionable social value.[133] Two other factors buttress this point. First, because of the Internet's globalizing function, domestic listeners now have more access to foreign speech than ever.[134] Second, First Amendment

---

130 564 U.S. 786, 786, 805 (2011).

131 559 U.S. 460, 461, 482 (2010).

132 *See* Thai, *supra* note 68, at 305 (noting that Supreme Court decisions "likely preclude the government from barring the entry of political speech from abroad . . . or that the speech is valueless or false . . . because the First Amendment demands an open marketplace of ideas for domestic listeners.").

133 United States v. Alvarez, 567 U.S. 709, 710 (2012).

134 *See* Thai, *supra* note 68, at 274 ("[T]he digitization and globalization of speech on the internet has made physical border restrictions largely irrelevant.").

doctrine emphasizes the listener's robust right to receive speech.[135] While foreign speakers cannot claim First Amendment protection,[136] prohibiting U.S. persons from accessing foreign speech violates the right to receive information and ideas.[137] As long as listeners—even if they are unwilling listeners—have the individual power to block the receipt of speech, the government cannot bar speech distribution on a wholesale basis as a method to protect listeners.[138] A listener's right to receive information does not depend on the speaker's nationality or from where the speech geographically originated.[139]

C. The Incitement Standard is Limited in the Internet Context

Some Russian disinformation tactics resemble fact patterns in incitement cases.[140] For example, an IRA-created page for a fake organization, "Heart of Texas," promoted a public protest of the Islamic Da'wah Center in Houston, specifically against the Center's opening of a new library. One comment urged, "Need to blow this place up. We don't need this [expletive] in Texas." Another IRA-created page promoted a "Houston Counter Against Hate." The pages planned a protest and counter-protest for the same day. The protesters on both sides fought verbally, but not physically.

However, First Amendment jurisprudence on incitement presents a high bar to censoring or criminalizing such speech. In *Brandenburg v. Ohio*,[141] the seminal Supreme Court case on the topic, the Court defined criteria for censoring speech. The Court held that a state may not prohibit any advocacy of the use of force or the violation of a law unless it is "directed to inciting or producing imminent lawless action and [it] is likely to incite or produce such

---

135 *Id.* (discussing the Supreme Court's First Amendment jurisprudence).

136 *Id.* at 276 ("[T]he Court has neither held nor assumed that foreign speakers abroad enjoy any First Amendment protection.").

137 Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U. L. REV. 1169, 1178 (2016) (noting that the marketplace of ideas theory "emphasizes the production of information regardless of source").

138 Thai, *supra* note 68, at 282.

139 *Id*.

140 Carolyn Y. Forrest, *Russia's Disinformation Campaign: The New Cold War*, 33 COMMC'NS. LAW. 2, Winter 2018, at 3 (discussing how the public was manipulated by Russian-linked content) (2018); *see also* BENKLER ET AL., *supra* note 20, at 263 (noting the disinformation campaign has orchestrated real-world rallies).

141 395 U.S. 444 (1969).

action."[142] The *Brandenburg* standard is only satisfied if someone explicitly urges serious, unlawful, and imminent conduct that is public and ideological.[143] Courts must consider the speech in context. The Court has applied *Brandenburg* only twice since 1969 and has continued to uphold a broad right to free speech.[144]

The imminence requirement of *Brandenburg* is difficult to apply to incitement on the Internet for three reasons. First, as John Cronan notes, words in the cyber-world are often "'heard' well after they are 'spoken,'" and are rarely heard by all readers simultaneously."[145] A provocative post would survive the *Brandenburg* standard because a disqualifying delay would likely occur between the time a reader or readers read the post and any unlawful action. Second, the speaker-audience relationship on the Internet is different than that imagined in *Brandenburg*. Internet posts are rarely designed for specific individuals and can easily spread across large and undefined audiences.[146] Third, it can be difficult to assess the intent standard behind an Internet post.[147] Recently, in *United States v. Carmichael*, a federal district court noted that, under *Reno,* "hostile speech disseminated to a broad audience should be treated as less threatening than speech directed to a specific person."[148] This suggests that incitement on the Internet may present less concern than what is said in person. Thus, the *Brandenburg* standard likely precludes the government from barring political speech from foreigners, even if it advocates lawless action, because of the imminence standard.

Some scholars have proposed modifying the incitement standard to encompass disinformation campaigns. John Cronan suggests a new incitement standard for the Internet involving four primary factors: "(1)

---

142 *Id*. at 447.

143 Clarified in *Hess v. Indiana*, "imminent" means that the speech must direct the action to happen right then. 414 U.S. 105, 108 (1973) (reversing the conviction of an antiwar demonstrator on the understanding that his statement did not advocate imminent or violent action). *See also* NAACP v. Claiborne Hardware Co., 458 U.S. 886, 929 (1982) (holding that when appeals to a crowd are protected speech when they do not incite lawless action).

144 *Hess*, 414 U.S. at 108; *Claiborne Hardware Co*., 458 U.S. at 927.

145 Cronan, *supra* note 95, at 428; *see also* Eugene Volokh, *The Freedom of Speech and Bad Purposes*, 63 UCLA L. REV. 1366, 1383 (2016) (discussing the *Brandenburg* opinion and its application to speech protection).

146 Cronan, *supra* note 95, at 426.

147 *Id.* at 443.

148 Lynn Adelman & Jon Deitrich, *Extremist Speech and the Internet: The Continuing Importance of* Brandenburg, 4 HARV. L. & POL'Y REV. 361, 369 (2010).

imminence from the perspective of the listener; (2) content of the message; (3) likely audience; and (4) [the] nature of the issue involved."[149] However, such a standard would likely raise First Amendment concerns. First, the *Brandenberg* standard considers imminence based on the intent of the speaker and the likelihood that the speech would cause imminent, unlawful action. Prior caselaw suggests that the Supreme Court would be unlikely to drop the requirement of the speaker's intent. Second, due to the unforeseeable reach of Internet postings, the audience that receives a post that imminently incites unlawful action may be different than that which the speaker initially intended.

Moreover, as Chen notes, modifying *Brandenburg* may be undesirable because of the rapidly-changing contexts of the Internet and national security.[150] Courts often show more deference to the State, even in the context of restrictions on civil liberties, during times of war or national security crises.[151] The current era of constant information warfare, plus the proximity in time of Russia's intervention in the 2016 elections, might lead to restrictions on free speech that would be undesirable in the long term. Thus, modification of the incitement standard in this manner is unlikely to be a good option for combatting disinformation.

Some literature suggests modifying the imminence requirement by attempting to show a "direct" link between online speech and the acts in question as well as considering the target audience and instructions given.[152] However, Michael Sherman argues that this is not an effective solution because it "would likely be limited to a relatively small number of situations in which a target could be pinpointed with some degree of specificity from the speech in question."[153] Changing the *Brandenburg* standard would not solve the jurisdictional and technological hurdles independent of First

149 Cronan, *supra* note 95, at 455.

150 Chen, *supra* note 99, at 380 (suggesting that "it is premature to reconstruct the *Brandenburg* test to address perceived changes in our global environment").

151 *Id*. at 386.

152 *See* Lidsky, *supra* note 118, at 161–62 ("[A] satisfactory replacement for imminence in cyber-incitement cases would focus on ensuring that the causal linkage between the speech and the harm was a direct one . . . ."); *see also* Russell L. Weaver, Brandenburg *and Incitement in a Digital Era*, 80 MISS. L.J. 1263, 1287 (2011) (noting that the *Brandenburg* approach was developed at a time before the Internet).

153 Michael J. Sherman, Brandenburg *v. Twitter*, 28 GEO. MASON U. CIV. RTS. L.J. 127, 138–39 (2018).

Amendment doctrinal concerns.[154] When considering the slippery-slope problem, changing this standard seems even more problematic. Moreover, online platforms like Facebook receive criticism for applying their current policies unfairly by favoring some groups over others.[155] As Sherman contends, while Facebook or Twitter "censorship" is vastly different from government censorship, there is a societal cost to "barring people from forums that are increasingly important to the exchange of ideas."[156]

D. Surveillance, Privacy, and the Chilling Effect

Restrictions on U.S. Government surveillance of U.S. persons also place the United States at an asymmetric disadvantage in fighting information warfare. Should the United States seek to regulate social media to prevent disinformation, it will need to surveil social media and other, similar platforms to discover the disinformation. However, government observation, monitoring, or censorship of U.S. persons threatens freedom of speech.[157] Oversight may result in a chilling effect on social media posts, which would raise fears of censorship in the new public square.[158] Fear of impingement on free speech, however, hampers the United States' ability to combat Russian influence campaigns.

1. 2018 Executive Order on Election Interference

In light of mounting evidence of Russian interference on the 2016 elections, President Trump issued an Executive Order on Election Interference in 2018.[159] However, this Order does not address the patchwork of U.S. surveillance laws that have prevented the intelligence

---

154 *Id.* at 162.

155 *Id.* at 163.

156 *Id.* at 164; *see also* Mark MacCarthy & Washington Bytes, *What Should Policymakers Do to Encourage Better Platform Content Moderation?*, FORBES (May 14, 2019, 3:57 PM), https://www.forbes.com/sites/washingtonbytes/2019/05/14/what-should-policymakers-do-to-encourage-better-platform-content-moderation/#14de817e1ee4 ("[D]eputizing platforms to remove legal material is a more general rule of law problem . . . .").

157 Howard, *supra* note 97, at 1367; *see also* BENKLER ET AL., *supra* note 20, at 386 (noting that there will likely be a substantial surveillance cost if there is "national security identification of foreign propaganda campaigns").

158 Howard, *supra* note 97, at 1368.

159 Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, Exec. Order No. 13,848, 83 Fed. Reg. 179 (Sept. 12, 2018).

community from preventing threats to the electoral process. The Order allows the intelligence community ("IC") to respond after election interference occurs, but not before. The Order provides that the Director of National Intelligence ("DNI") has forty-five days after the conclusion of a federal election to determine whether a foreign government or agent has "acted with the intent or purpose of interfering in that election."[160] The DNI will assess the nature of the interference, the methods of interference, the persons involved, and the foreign government(s) "that authorized, directed, sponsored, or supported it."[161] After receiving DNI's assessment, the Attorney General and Secretary of Homeland Security will provide the President and Secretaries of State, Defense, and Treasury with a report evaluating the extent to which the interference affected the security and integrity of the (1) election infrastructure[162] and results and (2) political organizations, campaigns, or candidates, if they were targeted.[163]

While the Order mentions that any actions by the intelligence community must respect First Amendment principles, it provides little guidance as to how the intelligence community can simultaneously collect intelligence relating to foreign interference in U.S. elections. Without addressing laws that restrict national security actors from conducting necessary surveillance to protect First Amendment freedoms, this executive order will do little to keep Russia and other foreign actors from influencing U.S. elections.

2. The Privacy Act

The Privacy Act of 1974 presents a formidable hurdle to combatting information warfare. The Act was passed following Watergate, at the height

160 *Id.* § 1(a). The DNI will make this determination in consultation with appropriate agencies.

161 *Id.*

162 The Order defines "election infrastructure" as "information and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results." *Id.* § 8(d). For discussion on how states and the Federal Government can improve the integrity of their election infrastructure, see the Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, S. REP. NO. 116-XX, at 54–61 (2019) (providing seven recommendations for improving cybersecurity in election infrastructure).

163 Exec. Order No. 13,848, *supra* note 159, § 1(b)(ii). The report will be generated in consultation with appropriate agencies and state and local officials. *Id.* § 1(b).

of public concern over abuse of government surveillance.[164] It regulates the government's collection, maintenance, use, and dissemination of personally identifiable information about individuals contained in federal agency record systems.[165] The Act seeks to protect individual privacy by preventing the unnecessary release or exposure of individual data.

The Privacy Act requires that the public can identify general national databases or "systems of records," which contain individually identifying information.[166] Individuals whose data is stored in these databases have the right to access, correct, or amend the information within it. The rules and regulations within the Privacy Act change depending on what type of agency is involved, the content of data, and how the data would be used.[167] The Act covers only databases from which an individual's data is retrievable using a personal identifier, such as a name or Social Security number.[168] Any information collected must be "relevant and necessary to accomplish a [required] purpose of the agency."[169] Furthermore, when an agency establishes or revises the "existence or character" of a database, it must publish a notice in the Federal Register describing the records and how the government may use them.[170]

---

164 William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099, 1110 (2007) (recounting the "various abuses by intelligence agencies, including NSA surveillance of Americans and drug traffickers, U.S. Army military intelligence surveillance of domestic groups, FBI covert operations against alleged subversive groups, CIA opening of domestic mail sent to or received from abroad, and electronic surveillance of political 'enemies'").

165 *See, e.g.*, Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (stating its purpose is "to amend title 5, United States Code, by adding a section 552a to safeguard individual privacy from the misuse of federal records, to provide that individuals be granted access to records concerning them which are maintained by federal agencies . . . .").

166 Statutory confidentiality guarantees prevent law enforcement agencies from accessing some databases, like Census Bureau databases. *See, e.g.*, 5 U.S.C. § 552a(a)(5) (2017); U.S. Dep't of Commerce, U.S. Census Bureau, *The "72-Year Rule,"* U.S. CENSUS BUREAU (last visited Oct. 20, 2019), https://www.census.gov/history/www/genealogy/decennial_census_records/the_72_year_rule_1.html ("The U.S. government will not release personally identifiable information about an individual to any other individual or agency until 72 years after it was collected for the decennial census."). The Privacy Act does not apply to this and other databases covered by specific confidentiality laws.

167 For instance, the Census Bureau is allowed to use personal records for statistical purposes. 5 U.S.C. § 552a(k)(4) (2017).

168 *Id.* § 552a(a)(5) (defining a "system of records" as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual").

169 *Id.* § 552a(e)(1).

170 Records, according to the Privacy Act, are:

When requesting data, federal agencies must clarify the authority under which the agency can solicit the information, and whether disclosing that information to the requesting agency is mandatory or voluntary.[171] This requirement serves as an additional check to ensure that information in the database is not freely accessed or accessed without cause by agencies. Agencies can access or acquire the information gathered and "donated" to the database only on a need-to-know basis.

The only category of sensitive data identified by the Privacy Act is personal data related to the exercise of First Amendment rights. Under section 552a(e)(7) of the Privacy Act, the government cannot maintain records of a U.S. person's First Amendment activities. In other words, the Privacy Act prevents a government agency from keeping a file about how someone exercises their right to free speech. The Act generally prohibits disclosure of any stored information—not just First Amendment information—without the written consent of the subject individual.

However, protection for the data related to First Amendment activities does not apply to "authorized law enforcement activit[ies]" and some CIA activities.[172] Law enforcement agencies like the FBI do not have a duty to disclose such collections. An agency may not have to obtain written permission if the disclosure is subject to one of twelve statutory exceptions. Notably, law enforcement agencies, or components thereof, that primarily perform criminal law enforcement duties need not make disclosures. The CIA may also exempt by rule any system of records it maintains, as explicitly provided for in 5 U.S.C. § 552a(j)(1).[173]

> [A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Id. § 552a(a)(4).

171 *Id.* § 552a(e)(3)(A).

172 *Id.* § 552a(e)(7); *see also* LEVINSON-WALDMAN, *infra* note 176, at 12 (discussing the misuses of the NSA's broad surveillance authority).

173 5 U.S.C. § 552a(j)(1) (2017) (authorizing the CIA Director to promulgate rules exempting documents from the access provisions of the Act); *see, e.g.*, Mobley v. CIA, 924 F. Supp. 2d 24, 55–56 (D.D.C. 2013) (finding records necessarily exempt from the disclosure provisions of the Privacy Act because they concern intelligence methods); *see also* 32 C.F.R. § 1901.62(d) (2019) (providing that individuals cannot access portions of the systems of records the CIA maintains that consist of or would reveal "intelligence sources or methods" and "documents or information provided by foreign, federal, state, or other public agencies").

The Act's purpose is to guarantee better protection of U.S. persons' privacy by limiting the circumstances in which their information is retained and shared.[174] Private litigation is the primary mechanism for legal oversight under the Privacy Act,[175] and government officials may be subject to criminal prosecution for certain violations of it.[176] However, the Act does not apply to data collected about persons outside the United States, nor does it protect the privacy of records that are maintained by the private sector or local or state governments.

The Privacy Act has been attacked from all sides. The DOJ has criticized the Act's imprecise language, limited legislative history, and outdated guidelines.[177] Some scholars and research organizations, like the Brennan Center for Justice, argue that the Act's exceptions for national security and law enforcement undermine its goals of protecting privacy. Rather than serving as a substantial check on government power to collect records, the Act functions as a "box-checking exercise."[178] Beyond the exceptions, gaps in the Privacy Act itself do not account for contingencies and potential threats to privacy. For example, the Act has no third-party privacy exemption to prevent the disclosure of information about the third party in another's file.[179] If Person *A* agreed to disclose information, the requesting agency could still use the data of Person *B* that exists in Person *A*'s file.

Most importantly for this Article's broader considerations, the law enforcement and nationality exemptions allow agencies to exempt

---

174 *See* LEVINSON-WALDMAN, *infra* note 176, at 49 n.413 (citing S. REP. NO. 99-1183, at 6916–18, 6920 (1974)).

175 5 U.S.C. § 552a(g) (2017).

176 *Id.* § 552a(i); *see also* RACHEL LEVINSON-WALDMAN, BRENNAN CENTER FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 12 (2013), https://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf (noting the misuses of the NSA's surveillance authority).

177 *Overview of the Privacy Act of 1974*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/opcl/introduction (last updated July 27, 2015).

178 LEVINSON-WALDMAN, *supra* note 176, at 49; *see also* Julia Angwin, *U.S. Terrorism Agency to Tap a Vast Database of Citizens*, WALL STREET J. (Dec. 13, 2012), https://www.wsj.com/articles/SB10001424127887324478304578171623040640006 (quoting an observation by a Privacy Act consultant to government agencies: "All you have to do is publish a notice in the Federal Register and you can do whatever you want.").

179 Evan M. Stone, *The Invasion of Privacy Act: The Disclosure of My Information in Your Government File*, 19 WIDENER L. REV. 345, 348 (2013) (discussing the dilemma that is faced when a person requests access to something under the Privacy Act, but the file also contains information about another person).

"databases from the provisions requiring transparency and an opportunity to challenge the accuracy of personal information,"[180] without detailed justification. The meaning of this provision is not entirely clear, but it seems to create a loophole for agencies that act in national security or law enforcement capacities to subvert the Act's protections on personal privacy and liberty, opening the door to a chilling effect on speech.

The knowledge that the government might be collecting one's Facebook posts could deter such posts being shared, thereby chilling free speech. The concern is not baseless. The Department of Homeland Security ("DHS") recently published notice of an update to its current system of record, which is regulated by the Privacy Act. This update, closed for comment on October 18, 2017, allows DHS to consider whether the social media presence of persons seeking to gain entry to the United States justifies refusal of a visa. The update also involves DHS storing social media data of immigrants with green cards, naturalized citizens, and permanent residents.[181] Another update allows DHS to source any information that is publicly available on the Internet on the record.[182] Under this update, DHS considers social media handles, aliases, search results, and associated information. Immigrants are not U.S. persons until they obtain green cards or citizenship, so DHS may legally collect data related to their First Amendment activity. However, these updates affect U.S. citizens who communicate with immigrants, who may self-censor out of fear that the government could use the information they convey with those overseas against them. Although the Privacy Act explicitly protects citizens and permanent residents, immigrants' social media data may include information about protected persons. In other words, U.S. citizens who interact with foreign visa applicants will have their data collected as third parties.

---

180 5 U.S.C. § 552a(j), (k) (2017); LEVINSON-WALDMAN, *supra* note 176, at 51.

181 It is unclear whether social media information collected during one's immigration process can be used *or* shared after one is naturalized. *See* Aleksander "Sasha" Danielyan, *EFF Urges DHS to Abandon Social Media Surveillance and Automated "Extreme Vetting" of Immigrants*, ELECTRONIC FRONTIER FOUND. (Nov. 16, 2017), https://www.eff.org/deeplinks/2017/11/eff-urges-dhs-abandon-social-media-surveillance-and-automated-extreme-vetting (explaining that information publicly available on the internet can be used by DHS for immigration enforcement purposes).

182 Notice of Modified Privacy Act System of Records, 82 Fed. Reg. 43,556 (Sept. 18, 2017), https://www.regulations.gov/document?D=DHS-2017-0038-0001 (providing notice that DHS is updating their Privacy Act System of Records).

Further, the Privacy Act does not regulate actions committed in the course of an FBI investigation, nor how data is documented in the investigation if the data is pertinent to authorized law enforcement activity. Requiring a blanket prohibition on surveillance and recording until "the agency was investigating a specific offense or a specific person"[183] would severely undermine agency activities. Therefore, as long as the law enforcement agency prepares documents for a law enforcement purpose, it will not violate the Privacy Act even if the agency references First Amendment activity.

Courts in Privacy Act cases have found that national security concerns generally prevail over concerns about the potential of the government's actions to chill speech—advertently or inadvertently—where collecting the information is "pertinent to and within the scope of a currently ongoing authorized law enforcement activity."[184] However, courts have upheld claims regarding the expungement of records that do not meet this standard. The Ninth Circuit case of Garris v. Federal Bureau of Investigation clarifies this standard.[185]

In *Garris*, the FBI had collected records and created memoranda regarding the plaintiff's Internet and social media activities.[186] The plaintiff argued that, under the Privacy Act, the FBI's collection of his First Amendment data was illegal, and that the Bureau's maintenance of these records in perpetuity was illegal because the records were not relevant to an active investigation.[187] The district court previously granted summary judgment for the FBI.[188]

In its decision, the Ninth Circuit drew a distinction between the maintenance of First Amendment data and the "incidental" collection of

---

183 MacPherson v. IRS, 803 F.2d 479, 484 (9th Cir. 1986).

184 Garris v. FBI, 937 F.3d 1284, 1294 (9th Cir. 2019) (emphasis added); *see, e.g.*, *MacPherson*, 803 F.2d at 484–85 (considering "the factors for and against the maintenance of such records of First Amendment activities on an individual, case-by-case basis" and holding the IRS and DOJ's maintenance of the appellant's protest speeches fell under the law enforcement exception because of their public nature); *see also* Bassiouni v. FBI, 436 F.3d 712, 718–19, 725 (7th Cir. 2006) (finding that the FBI did not violate the Privacy Act); Afifi v. Lynch, 101 F. Supp. 3d 90, 107 (D.D.C. 2015) (granting summary judgment because the records at issue complied with the Privacy Act).

185 *Garris*, 937 F.3d at 1300; Raimondo v. FBI, No. 13-cv-02295-JSC, 2016 WL 2642038, at *1–3 (N.D. Cal. May 10, 2016), *rev'd sub nom.* Garris v. FBI, 937 F.3d 1284 (9th Cir. 2019).

186 *Garris*, 937 F.3d at 1299; *Raimondo*, 2016 WL 2642038 at *11–16.

187 *Garris*, 937 F.3d at 1288.

188 *Id.*; *Raimondo*, 2016 WL 2642038 at *16.

First Amendment data pursuant to an authorized law enforcement activity.[189] Regarding the maintenance of data, the court held that "because the investigations underlying the Memos have concluded, the FBI's maintenance of the Memos is not pertinent to an authorized ongoing law enforcement activity and therefore violates the [Privacy] Act."[190] To meet its burden to show that records are pertinent to an authorized ongoing or future law enforcement activity, an agency must "articulate a sufficient law enforcement activity to which the maintenance of the record is pertinent,"[191] that is, presents a basis as to why the agency needs to continue to maintain it that is more than "speculative relevance."[192] Therefore, even where the original investigation leading to the collection of the records ends, an agency can still retain the record if it is "pertinent to an authorized law enforcement activity."[193] Since the record in question was not relevant to an ongoing law enforcement activity, the court held that the FBI must expunge the record, contrary to the lower court's determination.[194]

Although the Ninth Circuit required expungement of one of the memoranda related to the plaintiff's specific case, the Ninth Circuit left undisturbed the lower court's decision that an agency can retain records containing "incidental" collection of First Amendment information as long as the surveillance itself is relevant to an ongoing law enforcement activity.[195] The district court had recognized that the FBI's activities could potentially chill speech. However, it asserted that "[t]o forbid 'incidental' surveillance of innocent people or to require excision of references to such people in surveillance records would be administratively cumbersome and damaging

189 By "incidental" collection of data, the court refers to data collected during the FBI's observation and surveillance of plaintiff's website postings and other First Amendment activities. *Garris*, 937 F.3d at 1300. The term "incidental" is used in other cases, and colloquially, to refer to data about third parties collected as a result of law enforcement activity regarding other individuals. *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (2014) (describing that section 702 surveillance can result in the "incidental" collection of U.S. person communication where she communicates with a non-U.S. person who has been targeted). It is unclear whether the court accepts this broader usage.

190 *Garris*, 937 F.3d at 1294.

191 *Id.* at 1300.

192 *Id.* at 1299.

193 *Id.* at 1298.

194 *Id.* at 1300.

195 *Id.*; *see* Raimondo v. FBI, No. 13-CV-02295-JSC, 2018 WL 398236, at *1 (N.D. Cal. Jan. 12, 2018), *aff'd sub nom.* Garris v. FBI, 937 F.3d 1284 (9th Cir. 2019).

to the completeness and accuracy of the agency records."[196] Thus, the court interpreted the Privacy Act to allow "incidental" observation and collection of First Amendment data for valid law enforcement or national security reasons.[197]

III. REMEDIES

Free political speech is a cherished American freedom. Yet, prioritizing it has paradoxically led to an assault on U.S. values. As discussed above, U.S. law and Supreme Court doctrine constrain the United States' ability to fight disinformation campaigns. By upholding broad protections for both political speech and false speech, the Supreme Court created an environment in which Russian information warfare can flourish. Other laws meant to protect American freedoms, like the Privacy Act, paradoxically limit the United States' ability to protect the democracy that preserves those liberties. Scholars have proposed some solutions to these problems, such as modification of the incitement standard, use of counterspeech, and revision of current laws. However, these fixes are insufficient to solve the problem of disinformation campaigns.

The United States must fight information warfare on all fronts. Reforms to doctrine, laws, and policies are needed to protect national security. Congress and courts must be careful to balance civil liberties with the need to protect national security in the Internet age. Fortunately, many remedies for this First Amendment problem exist within current First Amendment doctrine. Others are discoverable through creative policies that comport with existing First Amendment principles, including legislation, regulation of online platforms, and voluntary actions by online platforms.

A. Doctrinal Remedies

1. Distinguish the Internet and Social Media Contexts

First Amendment jurisprudence must be reformed to account for the realities of the Internet and social media. This distinction is a prerequisite for modifying current Supreme Court jurisprudence on the Internet as the public square. As discussed above, the Supreme Court has tried to place the

196 *Raimondo*, 2018 WL 398236 at *16 (quoting MacPherson v. IRS, 803 F.2d 479, 484) (9th Cir. 1986).
197 *Id.* at *11–16.

Internet, broadly speaking, into the framework of the "new public square." This has led to a doctrine based on flawed intellectual assumptions. Courts should instead recognize the Internet and social media for the distinct legal animals that they are. A platypus should not be likened to other mammals while it is laying eggs. Similarly, the Internet and social media may be regulated when they behave in a manner distinct from traditional media and the public square, and the legal frameworks and doctrine that apply to them must be modified accordingly. This is especially critical when national security is at stake.

2. Distinguish the Electoral Context

Under current law, the U.S. Government might not have the legal authority to shut down, block, or mask First Amendment-protected speech by a U.S. person absent a clear showing that the U.S. person is operating as an unregistered agent of a foreign power. As detailed above, limitations on freedom of expression in the United States, such as libel and obscenity, are narrow and tightly controlled. Lies can be protected speech, especially when they relate to politics. Courts have ruled that the First Amendment protects statements about political candidates that are arguably false but non-defamatory, even if they seek to promote electoral interference.[198] Few circumstances exist in which the government is permitted to determine whether or not speech is truthful. As government activities increase in the domain of social media, it becomes more likely that the government will chill protected political speech, including political speech that is anti-government.

However, the electoral context may merit special constitutional protections. The First Amendment recognizes the primacy of political speech because of the importance of robust and free public discourse to a democracy. Six of our twenty-seven constitutional amendments focus on the expansion of the right to vote and clarification that the vote should not be suppressed on discriminatory grounds, reflecting that free and fair elections are fundamental to American democracy.[199]

---

198 *See* Susan B. Anthony List v. Driehaus, 814 F.3d 466, 476 (6th Cir. 2016) (holding that political false-statement laws were unconstitutional); Rickert v. Pub. Disclosure Comm'n, 168 P.3d 826, 831 (Wash. 2007) (holding unconstitutional a statute that prohibits a person from sponsoring a political advertisement containing a false statement); State *ex rel.* Pub. Disclosure Comm'n v. 119 Vote No! Comm., 957 P.2d 691, 699 (Wash. 1998) (holding a statute that prohibits sponsoring an advertisement with a false statement unconstitutional).

199 U.S. CONST. amends. XIII, XIV, XV, XIX, XXIV, XXVI.

When the right to free speech clashes with the freeness and fairness of the electoral process, it follows that speech freedoms that may not be abridged in other areas may be balanced against a societal interest in the integrity of the electoral process. Such restrictions might apply only to speech designed to threaten the integrity of the electoral process or to infringe upon the right to vote by suppressing turnout of certain groups. Laws need not restrict political speech in debates or other contexts previously considered in First Amendment cases.

Supreme Court jurisprudence on the First Amendment supports such a balancing test. *Packingham* left room for the government to regulate the Internet and social media if such regulation passes strict scrutiny.[200] Elsewhere, in *Brown v. Hartlage*, the Court recognized the state's "legitimate interest" in preserving the integrity of the electoral process.[201] The Court noted that this might be enough to justify some limitations on speech, so long as "the restriction operate[s] without unnecessarily circumscribing protected expression."[202] The government has a clear and compelling interest in protecting the constitutionally protected right to vote, necessary to satisfy the strict scrutiny standard. Thus, narrowly tailored legislation that limits some speech to protect the freeness and fairness of the electoral process or the right to vote might be constitutional. Such limitations on foreign individuals' speech are even more likely to survive strict scrutiny.[203] Constitutional protections are weaker for foreign individuals than they are for U.S. persons, especially as related to the electoral process, as will be discussed below.

The Court, moreover, has recognized that the government may permissibly limit defamatory, deliberate falsehoods, or speech made with reckless disregard for its truthfulness, because these types of speech may subvert the purposes of democratic government. In *Garrison v. Louisiana*, the Court held that the First Amendment restricts a state's power to impose criminal sanctions for criticism of official conduct of public officials, but left

---

200 Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

201 Brown v. Hartlage, 456 U.S. 45, 52 (1982).

202 *Id.* at 53–54.

203 This Article follows Supreme Court practice and uses the terms "foreign citizen" and "alien" interchangeably to refer to individuals who are not citizens of the United States. These terms do not include individuals who are dual citizens of a foreign country and the United States. The term "foreign national" covers foreign citizens except for lawful permanent residents (LPRs, commonly known as "green card holders." *See* 2 U.S.C. § 441e(b) (2002).

room for other regulation of falsehoods in the electoral context.[204] *Garrison* extended the *New York Times v. Sullivan* ("*Sullivan*") "actual malice" standard for defamation to the criminal context. In *Garrison*, a district attorney was convicted of criminal defamation for disparaging judges of the criminal district court during a press conference, with respect to a backlog of pending criminal cases.[205] The district attorney asserted that the backlog of cases was due to the "inefficiency, laziness and excessive vacations of the judges," which hindered his efforts to enforce vice laws, and said that the judges have "made it eloquently clear where their sympathies lie" regarding certain vice investigations.[206] The attorney was convicted under the Louisiana Criminal Defamation Statute, which permitted "a finding of malice based on an intent merely to inflict harm, rather than an intent to inflict harm through falsehood."[207] The Louisana Supreme Court found that the district attorney's statements impermissibly constituted an attack on the judge's character, rather than official conduct.[208] The U.S. Supreme Court reversed the Louisiana Supreme Court. The Court noted that falsehoods are constitutionally protected to ensure that freedom of speech is not chilled. The Court further held that the criticism was of official conduct as well as personal character, noting that "anything which might touch on an official's fitness for office is relevant."[209]

However, the Court noted that the *Sullivan* rule does not protect all political speech, nor all falsehoods. In the context of defamation, knowing and reckless falsehoods are not protected by the First Amendment.[210] A statute that criminalized an intent to inflict harm through falsehood—not just an intent to inflict harm—might be constitutional.[211] For a speaker to face civil or criminal liability under such a statute, the public official must "establish[] that the utterance was false and that it was made with knowledge

---

204 Garrison v. Louisiana, 379 U.S. 64, 67 (1964).

205 *Id.* at 65.

206 *Id.* at 66.

207 *Id.* at 73.

208 *Id.* at 76; *see also* Volokh, *supra* note 145, at 1391 ("*Garrison* came eight months after *New York Times v. Sullivan*, which famously required a mens rea as to falsehood: A defendant could only be held liable if the defendant knew or was reckless about the falsity of the accusation.").

209 *Garrison*, 379 U.S. at 77.

210 *Id.* at 73.

211 *Id.* at 74.

of its falsity or in reckless disregard of whether it was false or true."[212] The Court explained that:

> Although honest utterance, even if inaccurate, may further the fruitful exercise of the right of free speech, it does not follow that the lie, knowingly and deliberately published about a public official, should enjoy a like immunity . . . . That speech is used as a tool for political ends does not automatically bring it under the protective mantle of the Constitution. For the use of the known lie as a tool is at once at odds with the premises of democratic government . . . . Calculated falsehood falls into that class of utterances which "are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[213]

Garrison arguably allows speakers to be held liable in the defamation context for falsehoods that meet a high standard of intent. *Garrison* noted that a statute proscribing a private citizen's "intent to inflict harm through falsehood" in the electoral context might survive strict scrutiny.[214] This might apply to U.S. persons as well as foreigners. Thus, *Garrison*'s holding may extend to proscribe defamatory fake news or false speech designed to inflict harm through falsehood, or a coordinated campaign of falsehoods, when actual malice is present.

3. Restrict False Speech Designed to Skew Elections

Congress might also pass a narrowly tailored law that would prohibit false speech that is designed to attack the integrity of the electoral process. As mentioned above, the First Amendment protects false speech. *Alvarez* represents the U.S. Supreme Court's strongest statement of the importance of protecting falsehoods. However, *Alvarez* allows for a statute prohibiting knowing or reckless false speech intended to disrupt the integrity of a government process.[215]

Alvarez leaves room for placing knowing or reckless falsehoods outside of First Amendment protection. In overruling the Stolen Valor Act, the Court noted that the Stolen Valor Act targets falsity but nothing else.[216] Other

---

212 *Id.* at 74.

213 *Id.* at 75 (quoting Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

214 *Id.* at 73.

215 United States v. Alvarez, 567 U.S. 709, 710 (2012).

216 *Id.* at 718.

cases in which the Court has noted that false speech has no constitutional value, or less constitutional value than truthful speech, involved another type of legally cognizable harm associated with a false statement. For example, the Court has upheld statutes prohibiting false speech made in the context of fraud, or invasion of privacy.[217] The Court noted that in those cases, "the falsity of the speech at issue was not irrelevant to our analysis, but neither was it determinative."[218] The Court discussed instances in which restrictions on false speech are permissible, such as perjury statutes, which are unquestionably constitutional because perjured testimony obstructs justice because it can cause a court to make a judgment premised on falsehoods.[219] Moreover, statutes that prohibit falsely representing that one is speaking on behalf of the government, or that prohibit impersonating a government official, do not simply restrict false speech but protect the integrity of a government process.[220]

Thus, a narrowly tailored statute restricting speech intended to attack the integrity of the electoral process might pass strict scrutiny. Here, the false speech itself would not be constitutionally protected only where such speech is designed to ensure that elections are not free and fair. Under the test advanced in *Alvarez*, the government would have to be able to provide evidence that shows that the public's general perception of the integrity of the electoral process "is diluted by false claims" such as those at issue,[221] that counterspeech would be unable to "overcome the lie,"[222] and that less restrictive measures were unhelpful.[223] The Supreme Court would be more likely to uphold a statute restricting such speech by non-U.S. persons since constitutional protections are weaker when applied to foreigners. However, *Alvarez*'s rationale suggests that such speech by U.S. persons could be restricted as well.

Currently, the Supreme Court applies strict or exacting scrutiny to any legislation placing content-based restrictions on First Amendment freedoms. However, the Court must balance two competing First Amendment freedoms in its jurisprudence. An individual's First Amendment right to

---

217 *Id.*
218 *Id.* at 719.
219 *Id.* at 720–21.
220 *Id.*
221 *Id.* at 710.
222 *Id.* at 726.
223 *Id.* at 729.

political speech must be balanced against U.S. persons' First Amendment right to political expression through free and fair elections. Therefore, the Court should consider potential harm to American civil liberties from legislative restriction on an individual's right to disinformation versus potential harm to society from interference with the ultimate expression of U.S. persons' political speech via a free and fair electoral process. As noted above, in *Chaplinsky*, the Court justified restrictions on incitement because "such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[224] Following this standard, the Court might balance the social value of any disinformation "as a step to truth" against the social interest in free and fair elections.[225] Such a balancing test would be consistent with the Court's prior jurisprudence on free speech. The Court has held the right to political speech to be paramount precisely because of the importance of free and robust political discourse to self-government. It follows that protecting free and fair self-government would be a legitimate reason for restricting some speech. The Court has also excluded from First Amendment protection some types of speech that are likely to lead to tangible harm to individuals or society, like incitement to imminent lawless action or fighting words. Speech that is designed to undermine the integrity of U.S. elections is harmful not only to the right to self-government but also to national security. The Supreme Court should not always prioritize national security over civil liberties. However, the Court should not ignore national security concerns either, especially those that implicate constitutional concerns like free and fair elections. In considering legislation and efforts responding to disinformation campaigns, the Court must consider the overall context and intent of the campaign and response, rather than merely an individual's isolated act of speech.

The Supreme Court may also adopt a new standard for evaluating harmful, blatantly false speech. In his concurring opinion in *Alvarez*, Justice Breyer proposed an intermediate scrutiny approach in evaluating blatantly false speech that would replace the exacting scrutiny or strict scrutiny standards used in most free speech cases.[226] As described by scholar Jeffrey

224 Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

225 *Id.*

226 *Alvarez*, 567 U.S. at 732 (Breyer, J., concurring).

C. Barnum,[227] Breyer's test considers the harmfulness of targeted speech[228] and the potential constitutional harm in the regulation of the targeted speech.[229] The test also considers whether the government could have achieved its objective by less restrictive means.[230] Building on Breyer's approach, the Court could balance these factors to ensure that any statute regulating fake news and misinformation that is designed to skew elections does not create "disproportionate constitutional harm."[231] It could require the government to show that less restrictive means, such as counterspeech, would be insufficient to achieve the governmental interest.[232] In the online context, the government might have to show that online platforms are not taking sufficient steps to eradicate fake news or disinformation. Breyer's pragmatic approach is limited by the difficulty of evaluating the effectiveness of counterspeech as a remedy for fake news or disinformation designed to skew the electoral process. However, Breyer's approach presents a useful starting point from which to develop constitutionally permissible regulation of false speech.

4. Restrict Speech by Foreign Individuals in the Electoral Context

Restrictions narrowly tailored to prohibit threats to the electoral process by foreign individuals are especially likely to pass constitutional muster. First Amendment protections are most robust where U.S. persons engage in non-commercial speech, weaker when applied to foreign individuals inside the United States, and weakest when applied to foreign persons outside of the United States.[233] Foreign individuals within the United States can generally enjoy First Amendment freedoms of speech. However, the U.S.

227 Jeffrey C. Barnum, *Encouraging Congress to Encourage Speech: Reflections on United States v. Alvarez*, 76 ALB. L. REV. 527, 535–36 (2013) (deriving three major aspects of Breyer's intermediate scrutiny test).

228 *Alvarez*, 567 U.S. at 734–37.

229 *Id.* at 736.

230 *Id.* at 737.

231 *Id.* at 739.

232 *Id.*

233 *See, e.g.*, Bluman v. Fed. Election Comm'n, 800 F. Supp. 2d 281, 283 (D.D.C. 2011), *aff'd*, 565 U.S. 1104 (2012) (explaining limits of constitutional protections for foreigner individuals); Daniel Fried & Alina Polyakova, *Democratic Defense Against Disinformation*, ATLANTIC COUNCIL 4 (Feb. 2018), https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf ("First Amendment protections . . . seem weaker when applied to foreign persons, especially those outside the United States.").

Government may limit the rights of foreign individuals when it comes to distributing propaganda and participating in the electoral process.

The Supreme Court has permitted restrictions on speech that qualifies as foreign propaganda. In *Meese v. Keene*, the Supreme Court upheld a provision of the Foreign Agent Registration Act ("FARA") that required foreign agents seeking to distribute "political propaganda" within the United States to file with the Attorney General, report on the extent of dissemination, and label the material with the identity of the foreign agent and its registry with DOJ.[234] Foreign propaganda is defined as any communication from a foreign source intended to influence U.S. foreign policy. Because the Act only requires foreign agents to make disclosures that would allow the public to evaluate the propaganda better, the Court found that FARA's provision "place[d] no burden on protected expression."[235] Although FARA may not burden the content of the expression, it does place an additional restriction on the ability of foreign agents to make certain types of speech. Thus, *Meese* may leave an opening for additional regulation of speech by foreign agents, so long as it does not "burden protected expression." Under *Meese*, a requirement for registration of foreign agent-sponsored political advertisements or labeling of posts by foreign agents on social media platforms might be permissible.

A recent campaign finance case guides how foreign speech in the electoral context might be constitutionally regulated. In *Bluman v. Federal Election Commission*, the U.S. District Court for the District of Columbia upheld a federal statute barring foreign nationals staying temporarily in the United States from contributing to state and federal electoral candidates, contributing to national political parties and outside political groups, and making expenditures expressly advocating the election or defeat of a political candidate.[236] Per the Bipartisan Campaign Reform Act, the case was heard by a three-judge panel, then appealed directly to the Supreme Court, which summarily affirmed.[237]

Then-D.C. Circuit Court Judge Kavanaugh, writing for the three-judge panel, asserted that the government might bar foreign citizens, such as those

234 481 U.S. 465, 470–71, 485 (1987).

235 *Id.* at 480.

236 800 F. Supp. 2d 281, 283 (D.D.C. 2011).

237 *Id.* at 282.

who are not lawful permanent residents of the United States,[238] from participating in express advocacy in political campaigns or its functional equivalent if the foreign citizen's goal is to influence how voters cast their ballots.[239] In the campaign finance context, an express advocacy expenditure is one that funds "express campaign speech" or its "functional equivalent."[240] An advertisement is the "functional equivalent" of express advocacy if it "is susceptible of no reasonable interpretation other than as an appeal to vote for or against a specific candidate."[241] Kavanaugh highlights that express advocacy expenditures "finance advertisements, get-out-the-vote drives, rallies, candidate speeches, and the myriad other activities by which candidates appeal to potential voters."[242] Express advocacy is distinct from issue advocacy, or advocating for a particular political position or issue.

The court noted the thorny nature of the legal question at issue, which implicated both First Amendment rights and the strict scrutiny they ordinarily receive, and a matter of foreign affairs and national security that would ordinarily be subject to deferential rational basis review.[243] However, the court concluded that the statute would survive strict scrutiny, which meant that the court did not need to decide the appropriate standard of review.[244] After reviewing caselaw on the rights of foreign citizens in the United States, the court concluded that the caselaw reveals a "straightforward principle: It is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government."[245] Since political contributions and express-advocacy expenditures are an integral part of the U.S. electoral process, these campaign activities are part of the process of democratic self-government. Limiting foreign participation in the electoral process is "part of the sovereign's obligation to preserve the basic conception of a political community," of which foreigners are, by definition, not a part.[246]

---

238 *See* 52 U.S.C. § 30121(b) (2017) (defining foreign national for election contribution regulations).

239 *Bluman*, 800 F. Supp. 2d at 288.

240 Fed. Election Comm'n v. Wisconsin Right to Life, Inc., 551 U.S. 449, 456 (2007).

241 *Id.* at 469–70.

242 *Bluman*, 800 F. Supp. 2d at 288.

243 *Id.* at 285.

244 *Id.* at 285–86.

245 *Id.* at 288.

246 *Id*. at 287.

The court in *Bluman* specifically did not decide whether Congress could constitutionally extend the statutory ban on express advocacy by foreigners to lawful permanent residents. Nor did the court decide whether Congress could prohibit foreign nationals from engaging in issue advocacy and other speech outside contributions to candidates and parties, express-advocacy expenditures, and donations[247] to outside groups to be used for contributions to candidates and parties and express-advocacy expenditures. The court further cautioned the government that seeking criminal penalties for the statute would require proof of the defendant's knowledge of the law.[248]

Following *Bluman*, Congress could plausibly create legislation to ban foreigners from engaging in express advocacy in political campaigns. *Bluman* suggests that a ban on electoral participation by foreigners is permissible if its scope is limited to regulation of express advocacy or its functional equivalent. Under *Bluman*, it seems that the United States has a compelling interest in limiting the actions of foreign citizens in American self-government, including preventing foreign influence over the U.S. political process. However, no court has defined what it means for an operation to be "designed to influence our electoral process." In the campaign finance context, spending money on political advertisements is designed to influence the election. The same cannot be said as easily for social media posts and tweets.

Still, legislation prohibiting express advocacy by foreigners would not have prohibited all of the Russian disinformation campaigns. *Bluman* construed the foreign spending ban as express advocacy, but not issue advocacy. Issue advocacy is speech that does not expressly advocate the election or defeat of a specific candidate. Much of the Russian disinformation campaign involved disseminating false news about Hillary Clinton or magnifying societal divides about issues like police violence, which does not amount to express advocacy for the election or defeat of a particular candidate. Moreover, even a Russian-sponsored advertisement promising to

---

247 Foreign nationals cannot contribute to, or make expenditures in connection with, a U.S. election of any level. 52 U.S.C. § 30121 (2012); *see also* 11 C.F.R. § 110.20(i) (2019) (expanding regulation of the political expenditures of foreign nationals); Fed. Election Comm'n, Advisory Opinion 2000-17 (July 28, 2000), http://saos.fec.gov/aodocs/2000-17.pdf (barring domestic subsidiaries of foreign corporations from establishing political action committees if financed by a foreign parent company or if individual foreign nationals participate in its operations).

248 *Bluman*, 800 F. Supp. 2d at 292.

"Make America Great Again" might be considered issue advocacy depending on the context. Notably, the court in *Bluman* did "not decide whether Congress could prohibit foreign nationals from engaging in speech other than contributions."[249] *Bluman* thus cannot be read to support bans on lobbying or issue advocacy by foreigners.[250] However, *Bluman*'s reasoning that foreign citizens can be excluded from the activities of self-government to preserve a national political community suggests that additional restrictions on foreign nationals' participation in the electoral process may be appropriate.

To restrict these forms of political expression, Congress would have to show that the restriction furthers the compelling interest in preventing foreign influence over the U.S. political process and could achieve this goal at a cost that imposed a tolerable level of collateral damage to civil liberties. The legislation must be narrowly tailored so as not to include protected forms of speech. A balancing test to evaluate such legislation should consider the identity of the speaker, the intent of the speaker, the nature and extent of the restriction on speech, the type and potential gravity of harm to the electoral process, and the type and gravity of potential harm to the speaker if the speech were restricted.

As mentioned above, *Garrison* might permit the government to proscribe a private citizen's speech made with an "intent to inflict harm through falsehood" in the electoral context, regardless of whether the speaker is a U.S. person or a foreigner.[251] The unique characteristics of social media suggest that greater regulation of speech in the electoral context might be allowed irrespective of the speaker's identity. The Court must reconsider the balance of considerations that have produced its First Amendment jurisprudence. If the target of the legislation is a U.S. person, a different calculus applies because of potential restrictions on U.S. persons' civil liberties. If the target is a non-U.S. person, the balance of considerations would be different because constitutional protections are weaker for non-U.S. persons, especially if they are outside the United States.

---

249 *Id.*

250 *Id.*

251 *See* discussion *infra* p. 139.

5. A Note on Principal, Agent, and Attribution Problems

Although regulation of speech by foreigners in the electoral context may be constitutionally permissible, a question remains as to what counts as speech by foreigners. When a state does not overtly sponsor media outlets or actors, these entities fall into a legal gray zone. Online trolls, for example, fall into a gray area between individuals expressing their opinions and semi-organized non-state actors following a particular foreign state's political agenda.[252] The line between online activists' free speech and a foreign state's interference in elections, therefore, may be thin.[253] Attribution of an individual's conduct to a non-state actor can pose even more legal obstacles.

Further complications exist when information warfare is conducted by a foreign state using U.S. servers. For example, Russian actors conducted information warfare campaigns using U.S.-based servers. Intelligence collection in such a scenario would involve investigation of U.S. corporate property and possibly the collection of information about that corporation in addition to individual U.S. persons. A full discussion of the corporate legal issues and intelligence-related legal issues lies beyond the scope of this Article. However, this scenario highlights the complexities of the legal questions involved in combatting information warfare.

Another legal problem arises when considering foreign agents who are U.S. persons. *Bluman*'s holding is currently limited to foreign individuals. However, it is entirely foreseeable that an adversary state or non-state actor would employ U.S. persons in an information warfare campaign. Legislation designed to combat electoral interference would need to delineate limitations on their conduct.[254]

---

252 *See, e.g.*, Mike Wendling & Will Yates, *NATO Says Viral News Outlet is Part of "Kremlin Misinformation Machine"*, BBC NEWS (Feb. 11, 2017), https://www.bbc.com/news/blogs-trending-38936812 (discussing opposing views on independence of Russian-funded media outlet Sputnik); *see also* Andrew Higgins, *Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation*, N.Y. TIMES (May 30, 2016), https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html (reporting on harassment of journalist investigating Russia's "troll army").

253 EUR. PARL. ASS., DOC. 14523, LEGAL CHALLENGES RELATED TO HYBRID WAR AND HUMAN RIGHTS OBLIGATIONS, at 8 (2018), www.assembly.coe.int/nw/xml/XRef/XRef-DocDetails-EN.asp?fileid=24547 (follow PDF hyperlink) (noting that difficulties of accountability for online speech and problems attributing the speech of individuals to foreign states makes it challenging to determine what qualifies as freedom of expression versus foreign electoral interference).

254 *See* 50 U.S.C.A. § 1881a (2017), (listing, among other restrictions, that the government cannot intentionally target persons who are within the United States or U.S. persons (citizen or LPR), and any surveillance must be conducted consistent with the Fourth Amendment and the targeting and minimization procedures detailed in § 1881a(d) and (e)).

Any effective legislation that would protect the U.S. electoral process from foreign interference must be able to prohibit certain speech or conduct by agents of foreign adversaries. Yet, determining who qualifies as an agent of a foreign state is complicated, and determining who qualifies as an agent of a non-state actor is even harder. Any legislation created to address disinformation campaigns would be incomplete without specifying what link between principal and agent is required to restrict certain free speech rights.

B. Reforming Surveillance Laws

To succeed in the fight against information warfare, the U.S. Government will likely need to engage in some degree of surveillance of social media. To do so, it will need to modify its statutes involving surveillance of Americans' First Amendment activity. Congress must tread carefully when doing so in order not to repeat the mistakes of the PATRIOT Act, a major attempt to modify U.S. surveillance laws after 9/11.

1. Lessons from the PATRIOT ACT

Congress passed the PATRIOT Act shortly after 9/11 "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[255] The Act modified prior surveillance laws, setting new conditions under which the government could electronically monitor communications.[256] Newly legalized surveillance methods soon were applied domestically and were not used exclusively to combat terrorism. The Act was roundly criticized for weakening American civil liberties in the name of national security. By 2004, over 330 communities and 4 states passed resolutions formally objecting to the PATRIOT Act, primarily because of civil liberties concerns.[257]

Many critics saw the PATRIOT Act as an overbroad law that gave law enforcement agencies powers to surveil Americans for reasons having

---

255 USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 272 (2001) [hereinafter "PATRIOT ACT" or "the Act"].

256 Nathan C. Henderson, Note, *The Patriot Act's Impact on The Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 179 (2002).

257 John T. Soma et al., *Balance of Privacy vs. Security: A Historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285, 326–27 (2005) (citing *List of Communities that have Passed Resolutions*, ACLU, https://www.aclu.org/other/list-communities-have-passed-resolutions (last visited Oct. 23, 2019)).

nothing to do with fighting terrorism.[258] The Act was, in fact, used to surveil Americans for illegal activities other than terrorism.[259] Several provisions of the Act also allegedly violated First Amendment freedoms. For example, section 214 permitted the government to execute trap and trace orders against individuals so long as their activities were "not expressly within the First Amendment."[260] Critics argued that the term "expressly" could be interpreted narrowly, allowing government surveillance of a broad swath of speech.[261] The Act also altered the primary purpose for surveillance requirement: requests needed no longer assert that they had the primary purpose of intelligence gathering, but simply "a significant purpose."[262] Again, this increased the powers of law enforcement to surveil expressive activity for purposes other than fighting terrorism.

Additionally, the Act modified the Pen Register Act[263] to facilitate the government's compulsion of online platforms to conduct prospective envelope surveillance on its behalf, including records of dialing, routing, and signaling information.[264] The government would be able to see websites visited and subject lines of emails, with the standard of proof being a mere "relevant to an ongoing criminal investigation."[265] Critics argued that the Act abused civil liberties by only requiring minimal judicial review and not providing clear guidelines on how the intelligence community should avoid collecting content related to First Amendment Activity.[266] Congress amended some of the Act in response to these and other critiques.

---

258 For more discussion of the PATRIOT Act's flaws, see generally Kyle Welch, *The Patriot Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking*, 43 CAP. U. L. REV. 481, 481 (2015) ("When faced with [crises], the nation's democratically elected representatives have used disaster as fuel to propel previously unacceptable, even unconstitutional laws."); *see also* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U.L. REV. 607 (2003) ("The Act's surveillance provisions proved so controversial that Congress added a sunset provision.").

259 *See, e.g.*, *In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 448 (S.D.N.Y. 2005) (permitting grant of cell site information relevant to an ongoing criminal investigation involving the illegal sale of contraband pursuant to the combined authority of 18 U.S.C. § 3121 and the Stored Communications Act). The PATRIOT Act amended 18 U.S.C. § 3121. PATRIOT Act § 216.

260 Soma et al., *supra* note 257257, at 303 (citing PATRIOT Act § 214).

261 *See id.* at 303–04.

262 PATRIOT Act § 218.

263 18 U.S.C. §§ 3121–3127 (1986).

264 PATRIOT Act § 216.

265 *Id.*

266 Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 988 (2002).

Legislation to help combat information warfare would likely arouse even more controversy than the PATRIOT Act. Surveillance to fight information warfare would necessarily involve delving beyond "envelope information" into the content of electronic communications. In light of Supreme Court precedent and lessons learned from the PATRIOT Act, legislation that would increase government surveillance capabilities to fight information warfare must be carefully crafted to balance First Amendment rights and national security.

2. Improving Surveillance Laws and the Privacy Act

Legislation that would increase government surveillance capabilities must be narrowly tailored to achieve a specific national security purpose. The surveillance process must include checks to ensure that civil liberties are not violated. However, such checks must not be so onerous as to prevent agencies acting for a national security purpose from moving quickly to fight rapid and constantly changing information threats.

First, legislation must be tailored to specific national security concerns. Unlike the PATRIOT Act, the legislation must not become like a Christmas tree, where provisions with other purposes are attached without much connection, for other powers that law enforcement agencies and national security agencies would like to wield. The legislation must articulate a specific national security purpose that any related surveillance would support. For example, legislation could tailor the collection of data related to U.S. persons' First Amendment activities to collection related or incidental to national security and law enforcement efforts to protect U.S. elections against influence by foreign powers. Legislation must specify which agencies will conduct that surveillance, and what steps they will need to follow to gain permission to conduct that surveillance. To avoid previous problems associated with the Privacy Act, Congress should ensure that the legislation covers agencies beyond those who traditionally have law enforcement and intelligence-collection capacities. The legislation might include the DOS, DHS, and DOJ, given the necessity of a whole-of-government approach to fighting information warfare. Moreover, the legislation should contain a provision that allows arms of additional agencies to conduct necessary electronic surveillance on an expedited basis, without full amendment of the Act.

Legislators must build checks into the process to ensure that federal agencies are accessing U.S. persons' First Amendment information only for the aforementioned narrowly tailored national security purposes. The legislation should also grant the agencies the power to access only the information necessary to achieve the narrowly tailored and specified national security purpose. The legislation should require agencies first to research open-source data on U.S. persons whenever it is available and if time allows it to do so, given the potential urgency of a national security concern. Agencies should be required to get a court order or a warrant from a court of competent jurisdiction to conduct prospective envelope or content surveillance of Internet communications. A high threshold should be required to obtain the court order or warrant, along with stringent judicial review of the government's application. The court should issue the order only if the government can provide "specific and articulable facts" showing reasonable ground to believe that the content of the electronic communication is relevant and material to an ongoing investigation supporting the specific national security purpose.[267]

In this regard, the Foreign Intelligence Surveillance Act ("FISA") provides a useful model for allowing surveillance of foreign agents without unduly infringing on the civil liberties of U.S. persons.[268] For a judge to permit government surveillance under FISA, she must find probable cause that the target is a foreign power or an agent of a foreign power and probable cause that the facility is used by the target.[269] The judge may consider the target's past activities and any facts and circumstances relating to the target's current or future activities.[270] However, the judge cannot accept the government's assertion that someone is an agent of a foreign power solely based on activities protected by the First Amendment.[271] Because FISA

---

267 This language is derived from the Stored Communications Act. 18 U.S.C. § 2703(d) (1986).

268 *See generally* Jill I. Goldenziel & Manal Cheema, *Protecting First Amendment Rights in the Fight Against Disinformation: Lessons Learned from FISA*, 79 MD. L. REV. (forthcoming 2019) (arguing that the civil liberties protections embedded in FISA should be used and built upon in any legislation that requires access to U.S. persons' information to combat information warfare).

269 50 U.S.C. §1805(a) (2017).

270 *Id.* § 1805(b).

271 *Id.* § 1805(a)(2)(A); *see also* United States v. Aziz, 228 F. Supp. 3d 363, 376–77 (M.D. Pa. 2017) (holding that the judge could rely in part on these activities because the defendant's conduct exceeded "the bounds of the First Amendment's protective sphere"); United States v. Rosen, 447 F. Supp. 2d 538, 549 (E.D. Va. 2006) (holding that a judge can rely in part on these activities as long as there is probable cause that the target may be involved in unlawful clandestine activities).

forces the government to meet specific standards before an order based on an individual's First Amendment activities can be issued, FISA's provisions (50 U.S.C. §§ 1801–1885) are not so overly broad that they chill an individual's First Amendment rights.[272] That said, if the target of the surveillance is not a U.S. person or her activities are not protected by the First Amendment, a wiretap will not violate FISA if the target is labeled as a foreign power based solely on her First Amendment activities.[273]

A full and informed debate on any legislation or modifications to existing legislation is a must. This makes it especially important for Congress to act before a new presidential electoral cycle when the threat of imminent acts of information warfare could spur hasty legislation. Finally, a sunset clause within any legislation must be included to prevent adverse, long-reaching encroachments on civil liberties, especially ones that are unforeseen.

Congress should reform the Privacy Act along similar lines. It should expand the Act to allow agencies acting for a national security purpose, in addition to law enforcement agencies or agencies acting for law enforcement purposes, to access U.S. persons' communications. Once again, the DOS and the DHS should be added to the traditional list of law enforcement agencies, with a clause providing a process to allow the DOD to participate in exceptional circumstances,[274] and for additional agencies to participate without a revision of the bill. However, appropriate checks should be added to the process to prevent surveillance powers from becoming too broad. In

---

272 *See* United States v. Falvey, 540 F. Supp. 1306, 1314–15 (E.D.N.Y. 1982) (asserting that because the judge, not the Executive branch, makes the finding that the target is truly an agent of a foreign power, and that FISA admonishes that no U.S. person can be considered an agent solely based on her First Amendment activities, FISA is not overbroad); *see also* ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 471–72 (D.C. Cir. 1991) (explaining First Amendment limitations on FISA investigations).

273 *See* United States v. Megahey, 553 F. Supp. 1180, 1194–95 (E.D.N.Y. 1982), *aff'd mem.*, 729 F.2d 1444 (2d Cir. 1983) *and aff'd on other grounds sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984) (asserting that because no U.S. person was the target of the surveillance pursuant to FISA, the First Amendment caveat was not implicated); *see also* United States v. Sattar, No. 02 CR. 395 JGK., 2003 WL 22137012, (S.D.N.Y. Sept. 15, 2003) (upholding FISA determination of probable cause against First Amendment challenge based on activities not protected by the First Amendment).

274 *See* Exec. Order No. 12333 § 2.3(b), 46 Fed. Reg. 59,941(Dec. 4, 1981) (permitting intelligence collection on foreigners within the U.S. but not intelligence collection "undertaken for the purpose of acquiring information concerning the domestic activities of United States persons"); *see also id.* § 2.4 (requiring the IC to "use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad").

light of the potential for chilling speech, lawmakers should revisit the necessity of the current blanket exemptions for law enforcement and determine whether court orders and judicial review should be necessary at some steps in an investigative process.

Any laws allowing surveillance of U.S. persons' First Amendment activities must have adequate disclosure provisions. The DOJ's Digital Cyber Task Force Report outlines six situations in which information the Department collects concerning foreign influence operations may be disclosed to the general public. Three of them are to alert (1) unwitting recipients of covert support as necessary to assist in countering, (2) online platforms whose services are used to disseminate propaganda or disinformation, and (3) the public or other affected individuals, when doing so outweighs other countervailing concerns.[275] The DOJ asserts that disclosing influence operations to the public is a meaningful way to neutralize their effectiveness and mitigate their harm. These concepts were incorporated into Section 90.730 of Title 9 of the Justice Manual.[276] Disclosure of activities will only occur when the DOJ can attribute them to foreign sources with high confidence. However, the DOJ may choose not to disclose if such a disclosure would be counterproductive, such as inadvertently amplifying the message.[277]

These disclosure guidelines should be incorporated into any statute involving surveillance to fight information warfare. Since disclosure may interfere with an ongoing investigation, it will not always be possible to require national security actors to disclose when U.S. persons' First Amendment activities are being surveilled. However, agencies should be encouraged to make such disclosures when possible, especially with the purpose of actively engaging Americans in the fight against information warfare.

C. Sanctions

Sanctions may provide some deterrence against electoral interference. Section 2 of the 2018 Executive Order on Election Interference authorizes

---

275 CYBER DIGITAL TASK FORCE REPORT, *supra* note 6, at 16–17.

276 U.S. DEP'T OF JUST., JUSTICE MANUAL § 9-90.730 (2018), https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730.

277 *Id.*

sanctions against entities deemed to have engaged in election interference.[278] The Secretary of the Treasury may block their property under U.S. jurisdiction of foreign agents if they (1) "engaged in, sponsored, concealed, or otherwise were complicit in foreign interference," (2) "materially assisted, sponsored," or supported the election interference, or (3) "acted or purported to act for or on behalf of those whose property or property interests were blocked pursuant to the order."[279] Finally, section 3 allows the White House to implement sanctions and "any other measures authorized by law" beyond those who interfered and their facilitators, such as business entities.[280] The Secretaries of State and Treasury will recommend these sanctions to the President, alongside an assessment of the effect of these sanctions so that sanctions are "appropriately calibrated to the scope of the foreign interference identified."[281]

Sanctions may be a useful tool for fighting information warfare, and Congress may wish to consider expanding them. Their effectiveness is limited, however, by the difficulty of determining the source of election interference and the scope of that foreign interference. Moreover, retroactive sanctions like those in the Executive Order are punitive but inadequate to prevent electoral interference.

D. Fighting Foreign-Sponsored Paid Advertisements

The government can also regulate paid social media advertisements by foreign actors designed to influence the electoral process, just as it does on traditional media sites. For example, the government can require that any paid political advertisements include a clear statement of who paid for or is disseminating a message. Registration requirements for political users would be similar to those required for traditional media.

Following *Bluman*, any advertisement that "is susceptible of no reasonable interpretation other than as an appeal to vote for or against a specific candidate" would constitute express advocacy and therefore be prohibited by the BCRA.[282] Extending *Bluman*'s rationale, other forms of express advocacy by foreign actors can be prohibited altogether. Foreign-paid

278 Exec. Order No. 13,848, 83 Fed. Reg. 179 (Sept. 14, 2018).

279 *Id.* § 2(a).

280 *Id.* § 3(b).

281 *Id.*

282 Fed. Elections Comm'n v. Wisconsin Right to Life, Inc., 551 U.S. 449, 470 (2007).

advertisements designed to influence the electoral process that fall short of express advocacy can also be regulated. Such advertisements might be registered as propaganda and regulated accordingly. Foreign advertisers might also be required to disclose the source of the advertisement's funding, just as other U.S. advertisers are required to do when they post advertisements on particular electoral issues. Since legislation regulating paid political advertisements, whether paid for by foreigners or U.S. nationals, would be political speech and content-based, it must satisfy strict scrutiny. Such legislation must, therefore, be narrowly tailored to achieve a compelling state interest.

To satisfy the tailoring prong, legislation regulating paid online political advertisements must be drafted carefully so as not to be overbroad. The January 2019 case of *Washington Post v. McManus* illustrates the difficulties in creating a narrowly-tailored registration statute.[283] In *McManus*, a federal district court struck down Maryland's Online Electioneering Transparency and Accountability Act ("OETA") on First Amendment grounds. The OETA was enacted to help combat events like the 2016 Russian disinformation campaign. The Act required social media and news sites to self-publish an ad-buyer's identity and the total amount paid. The platform must post this information in a searchable format within forty-eight hours of the purchase, place it in a "clearly identifiable location" on the platform's website, and keep it there for at least one year following the relevant general election.[284]

Despite finding that the state had compelling interests in passing the statute, the court found that the legislation was not narrowly tailored. Citing *Bluman*, the court asserted that Maryland had compelling interests in preventing foreign governments and their nationals from interfering in their elections, informing voters about the source of online advertisements, and deterring corruption.[285] However, the statute was both over- and under-inclusive because it regulated more speech than is necessary and did not regulate the main tools that foreign operatives used to disrupt the 2016 elections.[286] The statute's publication requirement was most problematic

283 Wash. Post v. McManus, 355 F. Supp. 3d 272 (D. Md. 2019).

284 *Id.* at 283.

285 *Id.* at 298–99 (citing Bluman v. Fed. Election Comm'n, 800 F. Supp. 2d 281, 285–86 (D.D.C. 2011)).

286 *Id.* at 299.

because it compelled online platforms to post state-required information on their websites, ". . . treading on their First Amendment-protected interest in controlling the content of their own publications."[287] Further, the statute was redundant and unnecessary since Maryland campaign finance laws already prescribed less restrictive means of obtaining the same information.[288]

Moreover, the state inspection requirement was over-inclusive. The statute covered all online platforms, including news sites. However, no news site has been identified as having run a single foreign-sourced paid political advertisement.[289] Therefore, the Act was overbroad beyond its purpose of stopping foreign interference in elections because it included news sites in its ambit. The requirement also requires the media to enact the government's regulatory scheme, which is antithetical to the role of a free press that is meant to serve as a check on government excesses.[290] Finally, the Act did not advance its purpose. In particular, since the Act placed the burden on the advertisement's buyer to notify online publishers, a buyer could withhold notice. That would, in turn, absolve the publisher from disclosing information about the advertisement. An advertisement's buyer might also provide false information, and the publisher would be protected by the good-faith provision in the Act.[291] The Act's provisions thus did not target the foreign efforts that it purported to target and was not well-designed to catch foreign operatives.[292]

As of this writing, *McManus* is the only federal decision on legislation to regulate paid political advertisements in the wake of the Russian electoral threat. Several other state legislatures have passed similar legislation or have it pending.[293] *McManus* is currently being appealed.[294] It remains to be seen whether other courts will follow the Maryland District Court's approach. Learning from *McManus*, future drafters should avoid redundancy in campaign finance provisions and narrowly tailor the statute to achieving

287 *Id.* at 300.

288 *Id.*

289 *Id.* at 301.

290 *Id.*

291 *Id.* at 305.

292 *Id.* at 303–04.

293 *See* Democracy Protection Act, 2018 N.Y. Sess. Laws ch. 59, pt. JJJ (McKinney) (codified at N.Y. Elec. §§ 14-100, 14-106 to -107, 14-126); *see also* 2018 Wash. Legis. Serv. ch. 304 (West) (amending state campaign finance laws, including Wash. Rev. Code § 42.17A.005).

294 Wash. Post v. McManus, 355 F. Supp. 3d 272 (D. Md. 2019), *appeal docketed*, No. 19-1132 (Feb. 4, 2019).

specific goals. A given statute need not address every aspect of the Russian disinformation campaign; however, it must specify what aspects of information warfare the statute aims to combat, and how.

Other courts may not share *McManus*'s concern with requiring news and social media sites to post a reasonably short state-sponsored disclaimer or list of funders of paid advertisements, on their sites. To support its reasoning that such a requirement would violate press freedoms, *McManus* cited cases that forbade a state from requiring publishers to print content with which they did not agree. In our view, a government requirement for a publisher to print factually neutral information, such as a disclaimer or a list of advertisers, would not impinge on a publisher's editorial freedom.[295] The Federal Government requires paid political advertisements on traditional media to include appropriate disclaimers. To require a different standard for paid political advertisements online would be inconsistent with the Supreme Court's treatment of social media as similar to traditional media. Even if the Court were to distinguish social media and traditional media, as we have suggested above, disclaimers on political advertisements should not receive different First Amendment protections in online and television or print contexts.[296] If anything, disclaimers on Internet sites should be less onerous for an online publisher than they are for traditional media outlets, since space and timing are nearly unlimited commodities online while they are scarce in television and print media. Thus, states may be able to create legislation to regulate paid advertisements that are appropriately narrowly tailored to achieve a specific, compelling state interest.

E. Fighting Fake News

As discussed above, some fake news may be protected political speech. Jurisprudence does recognize the possibility that false speech by foreigners in the electoral context may not receive full First Amendment protection. The

---

295 The requirement in *McManus* would seem to be such a factually neutral disclaimer; the court does not elaborate on its reasoning for conflating a requirement of a publisher to provide facts contextualizing an advertisement with a requirement that editors publish content with which they may not agree.

296 Disclosure is required of "electioneering communications," which currently only covers broadcast, cable, or satellite television and does not include internet communications. 11 C.F.R. § 100.26 (2006); Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 368 (2010) (upholding disclaimer requirements).

Supreme Court should clarify this standard, and jurisdictions would do well to attempt to draft laws that would force courts to explore the right doctrinal balance between First Amendment freedom of speech and preserving the integrity of the political process.

However, defamation law provides an existing cause of action for those targeted by fake news stories, especially political candidates.[297] If fake news is "limited to *intentional or knowingly* false statements, it is reasonable to conclude that such statements would satisfy the intent requirement for defamation claims."[298] As discussed earlier, in *Garrison v. Louisiana*, the Court held that the heightened "actual malice" standard, as outlined in *Sullivan*,[299] applies to both civil and criminal libel cases. The statute may only punish false statements if made "with knowledge of their falsity or in reckless disregard of whether they are true or false."[300] The Court stated that the case they were considering did not consist solely of private defamation—which would require only a showing of negligence[301]—but public defamation because the statement was directed at a public official.[302] When harmful false publications of fact concern a public figure, the publisher must have acted with "actual malice."[303] In other words, the claimant must show that a false publication was made with a "high degree of awareness of . . . probable falsity."[304] "There must be sufficient evidence to permit the conclusion that the defendant in fact entertained serious doubts as to the truth of his publication."[305] Of course, such a statute must not prohibit satire or parody.[306] When considering *United States v. Alvarez*, it appears to be the case that "conscious falsehoods that cause legally cognizable harm are not

297 *See* Joel Timmer, *Fighting Falsity: Fake News, Facebook, and the First Amendment*, 35 CARDOZO ARTS & ENT. L.J. 669, 683–84 (2017) (explaining that the applicability of defamation law with regards to public officials is limited to circumstances involving malice).

298 David O. Klein & Joshua R. Wueller, *Fake News: A Legal Perspective*, 20 J. INTERNET L. 7 (2017) (emphasis in original).

299 N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (holding that a public official must present proof that the defamatory statement was made with knowledge or reckless disregard of its falsity).

300 Garrison v. Louisiana, 379 U.S. 64, 76–78 (1964).

301 The private plaintiff must normally establish that the false statement was made to a third party and it was of such a nature that it harmed or would tend to harm the plaintiff's reputation. RESTATEMENT (SECOND) OF TORTS §§ 558–559 (AM. LAW INST. 1977).

302 *Garrison*, 379 U.S. at 78.

303 *Id.*

304 *Id.* at 74.

305 St. Amant v. Thompson, 390 U.S. 727, 731 (1968).

306 *See* Hustler Mag., Inc. v. Falwell, 485 U.S. 46, 56–57 (1988) (finding that the statements were a parody of a public figure and therefore not published with actual malice).

protected," but unintentional false speech is protected even if there is cognizable harm.[307] Where there is consciously false speech with no legally cognizable harm, however, the speech is protected. Thus, "consciously false speech turns on an assessment of harm."[308] The speech must be knowingly or recklessly false and produce some legally cognizable harm to produce a successful defamation suit.

However, defamation laws have limitations in effectively combatting fake news or its harm. A person can only pursue defamation claims against fake news stories about themselves. In the electoral context, for instance, candidates who are the subject of defamatory fake news can pursue defamation claims against providers. To illustrate, Hillary Clinton could not bring a defamation claim against the story that the Pope endorsed Trump, even if it adversely affected her campaign. And the Pope, who could bring the claim, may be reluctant to do so for the time and expense involved as well as the fear of drawing more attention to the story.[309] The author of a defamatory statement may also be anonymous or live outside the jurisdiction of the United States, further impeding prosecution.[310] Finally, a defamation lawsuit is unlikely to be resolved before the election, so readers will not be informed of the veracity of the "news" promptly.

Moreover, section 230 of the CDA protects interactive online providers from defamation claims where the information was "provided by" another Internet user.[311] Under traditional defamation law, a publisher can be liable for defamatory statements without their knowledge of the statement's inclusion.[312] But, with section 230, online providers have "federal immunity to any cause of action that would make service providers liable for

---

307 Martin H. Redish & Kyle Voils, *False Commercial Speech and the First Amendment: Understanding the Implications of the Equivalency Principle*, 25 WM. & MARY BILL RTS. J. 765, 792 (2017); *see also* United States v. Alvarez, 567 U.S. 709, 718–19 (2012) (discussing the protection of false speech under the First Amendment).

308 Redish & Voils, *supra* note 307, at 793.

309 *See* Timmer, *supra* note 297, at 685–86 (explaining barriers for defamation plaintiffs).

310 *See* Andrea Butler, Note, *Protecting the Democratic Role of the Press: A Legal Solution to Fake News*, 96 WASH. U. L. REV. 419, 436 (2018) (explaining barriers for defamation plaintiffs).

311 47 U.S.C. § 230(c)(1) (2017); *see also* Klein & Wueller, *supra* note 298, at 7 (noting, however, "the CDA does not afford protection to the original author of a defamatory or otherwise tortious publication"); Timmer, *supra* note 297, at 687-88 (discussing the barrier § 230 poses to defamation plaintiffs).

312 *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (discussing the state of the law prior to the enaction of the CDA).

information originating with a third-party user of the service."[313] Thus, if the website "does not contribute to the development" of the fake news, it cannot be liable for the defamatory statements posted by third parties.[314]

Defamation statutes may still provide some utility in fighting fake news. For a defamation statute to regulate fake news or misinformation, it must specifically identify the harm "that falls outside what is already actionable."[315] A statute that did not identify such specific harm would have the potential to limit First Amendment freedoms.[316]

F. Fighting Divisive Propaganda

Of the three main tactics of the Russian disinformation campaign, divisive propaganda is the hardest to fight. As discussed above, much divisive propaganda is protected by the First Amendment as political speech. Changing Supreme Court doctrine to allow regulation of foreign speech in the electoral context, following the suggestions above, will help fight divisive propaganda. However, laws that restrict government surveillance of the First Amendment activities of U.S. persons still pose a large hurdle to fighting divisive propaganda. These laws must be reformed to allow the U.S. Government to find and prosecute those undermining the U.S. electoral process while still protecting the civil liberties of U.S. persons.

1. Reforming the Foreign Agent Registration Act

FARA has the potential to help fight information warfare. Given First Amendment protections, the United States probably cannot ban media outlets that are overtly sponsored by foreign states—even if they are disseminating extremist or disruptive propaganda. However, the United States can identify them as "propaganda vehicles" and require them to

313 *Id.* at 330; *see also id.* ("[L]awsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.").

314 *See* Butler, *supra* note 310, at 433 (noting that "[a]ll federal courts to consider the issue . . . have followed . . . this precedent").

315 *See* Dallas Flick, Comment, *Combatting Fake News: Alternatives to Limiting Social Misinformation and Rehabilitating Quality Journalism*, 20 SMU SCI. & TECH. L. REV. 375, 396 (2017) (discussing the challenges of creating a law narrow enough to survive First Amendment scrutiny).

316 *Id.*

register under FARA.[317] Under FARA, acting as an agent of a foreign power requires registration and doing so without registration can be criminal.

FARA requires persons who act as agents of foreign principals to make periodic public disclosure of their relationship with the foreign principal.[318] The agent must also disclose their activities, receipts, and disbursements that are in support of those activities.[319] A willful violator may be subject to fines and imprisonment.[320] If the violator is an alien, they may be subject to deportation.[321] As the Cyber Digital Task Force Report states, "[o]vert influence efforts by foreign governments . . . may not be illegal, provided they comply with [FARA]."[322] However, FARA also enables the government to watch companies that register as agents of foreign adversaries more closely by putting U.S. agencies on notice of their work.

The DOJ has recently stepped up its enforcement efforts against entities that have not fulfilled their FARA obligations.[323] The Department is now educating prosecutors and agents on how to investigate criminal violations of FARA, expanding outreach to those who may be required to register, and compelling registration of those who are not in compliance, including American agents of Russian state-funded media networks.[324] However, FARA enforcement is historically difficult, given its numerous exceptions and the difficulty of navigating its broad language.[325]

Furthermore, the Department has moved to pursue criminal cases. It unsealed a criminal complaint of conspiracy on October 19, 2018, against Elena Alekseevna Khusyaynova, who is alleged to be the chief accountant of the Russian operations to influence the 2016 presidential election and 2018

317 *See* Fried & Polyakova, *supra* note 233, at 5 (discussing the DOJ's attempt to register RT as such).

318 22 U.S.C. §§ 611–21 (2017).

319 *Id.* § 612.

320 *Id.* § 618(a).

321 *Id.* § 618(c).

322 CYBER DIGITAL TASK FORCE REPORT, *supra* note 6, at 6.

323 *Id.* at 11.

324 *Id.*

325 The exemptions, among others, include those who engage in political activities, act in a public capacity, engage in certain business activities, engage in academic or scholastic pursuits, lawyers, and represent the interests of a foreign principle before the U.S. Government. 22 U.S.C. § 613 (2017). *But see* OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, AUDIT OF THE NAT'L SEC. DIV.'S ENF'T AND ADMIN. OF THE FOREIGN AGENTS REGISTRATION ACT (2016) (calling for better DOJ enforcement of FARA); Katie Benner, *Justice Dept. to Step Up Enforcement of Foreign Influence Laws*. N.Y. TIMES (Mar. 6, 2019), https://www.nytimes.com/2019/03/06/us/politics/fara-task-force-justice-department.html (reporting on increased enforcement of FARA).

midterm elections.[326] The government claimed it had probable cause to believe that Ms. Khusyaynova violated a criminal conspiracy statute[327] and obstructing enforcement of FARA and the Federal Election Campaign Act.[328] The complaint was released three weeks before the 2018 midterm election, despite DOJ policy not to take major steps on politically sensitive matters just before an election.[329]

FARA remains an avenue requiring legislative reform,[330] including the need for DOJ's National Security Division to have the authority to compel the production of records from registrants and updating the Act's definition to cover the digital age. Updating FARA is only part of ensuring transparency as to the identity of foreign agents.

2. Register and Regulate Bots

Legislation to regulate bots can also help fight information warfare. Congress might consider laws making it illegal for bots to deceive people about their identity for the purposes of influencing elections. California is leading the way in this area, passing a law in September of 2018 that makes it illegal for a person to use a bot:

> with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot.[331]

The law further requires a disclosure that is "clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts that it is a bot."[332] It does not impose a duty on service providers of

---

326 Victoria Clark et al., *Russian Electoral Interference: 2018 Midterms Edition*, LAWFARE (Oct. 19, 2018, 7:36 PM), https://www.lawfareblog.com/russian-electoral-interference-2018-midterms-edition [hereinafter *Russian Electoral Interference*].

327 18 U.S.C. § 371 (2018) (criminalizing conduct by which "two or more persons conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose" and "one or more of such persons do any act to effect the object of the conspiracy").

328 *Russian Electoral Interference*, *supra* note 326.

329 *Id.*

330 *See, e.g.*, Disclosing Foreign Influence Act, S. 2039, 115th Cong. (2017). The bill would enhance FARA enforcement and compliance by allowing the DOJ to issue Civil Investigation Demands, require the DOJ to develop a FARA enforcement strategy, and eliminate the registration exception created by the Lobbying Disclosure Act of 1995.

331 2018 CAL. STAT. 92 (enacted).

332 *Id.*

online platforms, such as social media sites. If successful, such bot disclosure laws would help avoid some source-credibility issues in misinformation campaigns. However, it remains to be seen whether such laws can be enforced effectively in a rapidly changing online environment.

Bot registration laws might be more effective. A person using a bot to influence an electoral vote might have to register the bot to do so, alerting the government or the online platform to the bot's presence and intended behavior. Automated bots do not necessarily have First Amendment rights. However, when a person is behind the bot, First Amendment concerns may still be implicated in any surveillance of those bots. Since humans control bots in varying degrees, with some bots nearly autonomous and others involving substantial human control, regulation of bots falls into a thorny constitutional gray zone.

3. Prosecute Operatives Who Target the Right to Vote

The United States can also combat Russian information warfare by investigating and prosecuting operatives who seek to infringe upon U.S. citizens' right to vote. Congress can enact legislation criminalizing information campaigns that are designed to suppress the vote. To ensure protection for freedom of speech, Congress must carefully define a standard for distinguishing information campaigns designed to suppress the vote from other political speech. Congress should require proof of intent to suppress the vote and identification of a targeted group of voters whose vote a campaign is designed to suppress. The Fifteenth Amendment, related constitutional amendments that support the right to vote, and the Voting Rights Act would support such legislation.[333] The legislation would advance the compelling state interest of protecting the U.S. electoral process against foreign interference. These constitutional amendments forbid state action that would suppress the right to vote, not private action. However, state inaction that allowed suppression of the right to vote would run counter to the spirit of these amendments when such state action is possible.

Criminalizing disinformation campaigns targeting the voting process would send a powerful signal to U.S. enemies and those acting on their behalf, including U.S. persons. The existence of criminal laws against disinformation campaigns that target the right to vote may cause trolls and

333 *See* U.S. CONST. amends. XIII, XIV, XV, XIX, XXIV, XXVI; Voting Rights Act of 1965, 42 U.S.C. § 1973 (2017) (protecting the individual right to vote in different ways).

others to refuse to participate in Russian disinformation campaigns. Sanctions on or punishment of those who disobey the laws will provide a further deterrent. The existence of laws criminalizing private voter suppression would also signal to the American public that voter suppression will not be tolerated. Such laws will also signal that the Federal Government seeks to encourage voting by African Americans and other historically marginalized groups. If such encouragement increases voter turnout, democratic values will prevail over attempted foreign interference.

4. Employing and Improving Counterspeech

As discussed above, the counterspeech doctrine rests on a shaky intellectual foundation when considering what we now know about human psychology and the modern marketplace of ideas.[334] Since news consumers are likely unable to gauge the validity of the reporting properly, counterspeech may do little to ensure that truth prevails or improve the quality of democratic decision-making.[335]

Counterspeech may still be a valuable tool in counterpropaganda efforts under certain conditions. More research is needed to determine how best to muster government resources in support of useful counterspeech efforts to fight information warfare. Also, the U.S. Government must be careful not to get into the business of determining what is true and what is false. If disinformation exists about government programs themselves, the United States is free to refute it. The government might counter falsities about access to elections or voter registration, for example. However, if, for instance, fake news is being spread about political candidates, the government must not be the arbiter of whether that news is true or false so as not to censor speech.

Based on the above analysis, U.S. counterspeech efforts should avoid the firehose approach and carefully target programs toward its audience. The United States would do well to promote the importance of assessing the credibility of news sources and warn consumers before misinformation occurs or immediately thereafter. This would help combat the problem of the resilience of first impressions. The United States should also make and

334 *See* Ho & Schauer, *supra* note 103, at 1167–75 (examining human psychology and the marketplace of ideas). *See generally* MARI J. MATSUDA, *Public Response to Racist Speech: Considering the Victim's Story*, *in* WORDS THAT WOUND: CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT 17, 48 (Mari J. Matsuda et al. eds., 1993).

335 Napoli, *supra* note 1, at 82.

repeat public announcements dispelling political statements that are disinformation in order to make the public familiar with the truth. However, the United States must be careful to frame its retractions in such a way as not to repeat an original false news story and breed familiarity with it. The United States should also develop correct counternarratives after falsities are removed, both to elevate the truth and to ensure that consumers understand how to avoid falsehoods in the future.[336] In engaging in this messaging, it is critical that the U.S. Government does so with attribution, so it is clear to recipients who is the source of information.[337]

Most importantly, the United States must be proactive and work to stop information warfare at its source.[338] The Pandora's box of false news can cause irreparable damage from the moment it is opened. Falsehoods may not even become entirely apparent until long after the speech is made and the damage is done.

For this reason, counterspeech efforts must work toward removing the sources of false speech themselves. Counterspeech efforts must focus on identifying, and training others to identify, fake news and fake news outlets and exposing or eradicating them. Geltzer and Kupchan suggest a U.S. Government-sponsored "information campaign" to make the public aware of Russian information warfare.[339] They argue that greater awareness that the Kremlin is deliberately seeking to pit Americans against themselves can help make the public less susceptible to manipulation.[340] Similarly, Joseph Thai argues for a K–12 media literacy curriculum to teach students to evaluate the quality and credibility of sources.[341] More research is needed to

---

336 Paul & Matthews, *supra* note 25, at 10.

337 The U.S. Government has always put forth its own messaging, with attribution, e.g., agency social media accounts and counter-messaging efforts abroad, per statutes like Smith-Mundt. *See, e.g.*, 22 U.S.C. §§ 1431–1442(a) (2018).

338 Paul & Matthews, *supra* note 25, at 10.

339 Joshua Geltzer & Charles Kupchan, Opinion, *What Counterterrorism Can Teach Us About Thwarting Russian Disinformation*, WASH. POST: DEMOCRACYPOST (Feb. 22, 2018), https://www.washingtonpost.com/news/democracy-post/wp/2018/02/22/what-counterterrorism-can-teach-us-about-thwarting-russian-disinformation/.

340 *Id.* U.S. efforts to counter Soviet propaganda during the Cold War might be useful to draw on. *See generally* Ashley Deeks et al., *Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?*, LAWFARE (Oct. 25, 2017, 7:00 AM), https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts (discussing the range of strategies the U.S. used to combat Soviet propaganda).

341 Thai, *supra* note 68, at 319.

determine whether these efforts are effective at promoting a well-informed democratic populace.[342]

a. The Revised Smith-Mundt Act

The United States recently modified its laws to allow the DOS to conduct more foreign-directed counterspeech. Before 2012, the effectiveness of the U.S. Government's response to disinformation campaigns was hindered by the U.S. Information and Educational Exchange Act of 1948,[343] also called the Smith-Mundt Act. Congress initially enacted the Smith-Mundt Act to counter the worldwide communist propaganda released by the Soviet Union during the Cold War. It outlined the United States' plan to "promote a better understanding of the United States in other countries, and to increase mutual understanding between the people of the United States and the people of other countries."[344] The Act permitted the U.S. Government to disseminate such messages abroad.[345] However, the Act prohibited the dissemination of U.S. influence information to U.S. persons, or within the United States.[346] As with the Privacy Act, Congress wanted to resist parallels drawn between Soviet propaganda efforts and U.S. actions.[347] Therefore, Congress designed restrictions to prevent foreign-bound information from being distributed or accessible to the American public.[348]

In 2012, Congress amended the Smith-Mundt Act, recognizing the impossibility of restricting Americans from accessing information designated for foreign audiences in the Internet age. Congress removed the domestic dissemination ban, thereby allowing government material produced for overseas consumption to be made available to the American public.[349] Both

342 *See* Lazer et al., *supra* note 27, at 1095 (discussing the "surprisingly few scientific answers" to questions about fake news and its impact); Timmer, *supra* note 297, at 705 (describing Facebook's Journalism Project).

343 22 U.S.C. §§ 1431–1442(a) (2017).

344 *Id.*

345 Weston R. Sager, Note, *Apple Pie Propaganda? The Smith-Mundt Act Before and After the Repeal of the Domestic Dissemination Ban*, 109 NW. U. L. REV. 511, 519 (2015).

346 *See id.* (arguing a de facto ban existed).

347 *See* Allen W. Palmer & Edward L. Carter, *The Smith-Mundt Act's Ban on Domestic Propaganda: An Analysis of the Cold War Statute Limiting Access to Public Diplomacy*, 11 COMM. L. & POL'Y 1, 11 (2006) (quoting Senator Edward Zorinsky, "[t]he American taxpayer certainly does not need or want his tax dollars used to support U.S. Government propaganda").

348 Sager, *supra* note 345, at 519.

349 *Id.* at 528.

the Senate and the House passed the amendment in late 2012,[350] and on January 3, 2013, President Obama signed the legislation into law.[351]

The amended Smith-Mundt Act provides the DOS with an improved tool to fight information warfare through counterspeech. The DOS is now able to target diaspora communities susceptible to the anti-American propaganda streaming into the United States.[352] The amendment was designed to include other checks to ensure that the U.S. Government still does not propagandize its people in a manner comparable to the former Soviet Union.[353] While U.S. persons can now access and judge State-created propaganda, the DOS cannot aim to influence U.S. public opinion directly. For example, programming comes from the Broadcasting Board of Governors ("BBG"), which is independent of the DOS and known for its excellence in journalism.[354] The DOS and the BBG specifically[355] may not disseminate their materials to U.S. citizens on their own volition but may only make them "available" to those who wish to access them.[356] The DOS and the BBG also may not create programming intended for a domestic audience or broadcast programming within the United States before disseminating it abroad.[357] In other words, although the DOS and the BBG may broadcast their programming within the United States, the American people can be neither the intended nor the initial audience.[358] The most meaningful restriction on the domestic dissemination is likely the DOS's appropriations bill, which contains a provision prohibiting the agency from disseminating "propaganda" within the United States without the

350 National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, 112th Cong. § 1078 (2013).

351 *See* Press Release, The White House, Office of the Press Sec'y, Statement by the President on H.R. 4310 (Jan. 3, 2013) (announcing signature of the authorization act).

352 Rebecca A. Keller, Influence Operations and the Internet: A 21st Century Issue 11 (Feb. 17, 2010) (unpublished manuscript) (available at https://apps.dtic.mil/dtic/tr/fulltext/u2/1018557.pdf).

353 *See, e.g.*, Rosa Brooks, *The Case for American Propaganda*, FOREIGN POLICY (July 17, 2013, 10:35 PM), https://foreignpolicy.com/2013/07/17/the-case-for-american-propaganda/.

354 BROADCASTING BOARD OF GOVERNORS, BBG STRATEGIC PLAN 2018-2022, INFORMATION MATTERS: IMPACT AND AGILITY IN U.S. INTERNATIONAL MEDIA (2018), https://www.usagm.gov/wp-content/uploads/2018/02/BBG-Strategic-Plan-2018-2022_FINAL.pdf.

355 National Defense Authorization Act for Fiscal Year 2013, H.R. 4310, 112th Cong. § 1077 (2012).

356 Sager, *supra* note 345, at 529.

357 22 U.S.C. § 1461–1a(a) (2013) (clarifying that the DOS and the BBG cannot use funds "to influence public opinion in the United States"). However, the DOS or BBG may communicate, "either directly or indirectly," regardless of whether "a United States domestic audience is or may be thereby exposed to program material." *Id.* § 1461-1a(b).

358 Sager, *supra* note 345, at 532.

authorization of Congress.[359] The United States Government Accountability Office defines propaganda as (1) self-aggrandizing, (2) purely partisan, or (3) covert.[360] Critics argue that these restrictions are insufficient to ensure that U.S. persons are not propagandized. For example, U.S. Government programs can easily be misappropriated and rebroadcast by individuals, regardless of the audience for which the programming was designed.[361]

Moreover, even the most innocent DOS or BBG programming could be considered covert propaganda if, without congressional approval, it is "circulated as the ostensible position of parties outside the agency"[362] through "surreptitious means."[363] Therefore, if the unattributed programming is impossible to verify or activities merely influence public emotions, such as by placing the U.S. flag behind a government spokesperson, government agencies may legally distribute it.[364] Scholar Weston Sager concludes that an agency violates the covert propaganda prohibition if the intended audience cannot ascertain the proper source of the government-produced materials.[365]

The 2012 amendment to the Smith-Mundt Act was a necessary tool to allow the government to fight information warfare. Given modern technology, any efforts by the U.S. Government to distribute information risk misappropriation. The government will have to develop tactics, legal and otherwise, to avoid misappropriation of its propaganda. It will also need to continue to comply with other restrictions on intelligence collection and privacy, as discussed above.

---

359 *See, e.g.*, Consolidated Appropriations Act, 2012, Pub. L. No. 112-74, § 7055, 125 Stat. 786, 1243–44 (2011) (restricting any appropriation from the Act from being used for propaganda purposes without Congressional authorization).

360 KEVIN R. KOSAR, PUBLIC RELATIONS AND PROPAGANDA: RESTRICTIONS ON EXECUTIVE AGENCY ACTIVITIES 6 (2005); 1 OFFICE OF THE GEN. COUNSEL, U.S. GEN. ACCOUNTING OFFICE, PRINCIPLES OF FEDERAL APPROPRIATIONS LAW 4-197 (3d ed. 2004) (describing how appropriation acts commonly prohibit the use of funds for propaganda, which is often defined "though administrative interpretation").

361 Sager, *supra* note 345, at 532–33.

362 *Id.* (citing OFFICE OF THE GEN. COUNSEL, *supra* note 348, at 4-202).

363 KOSAR, *supra* note 360, at 7.

364 *Id.*

365 Office of Nat'l Drug Control Pol., B-303495, 2005 WL 21443, at *4 (Comp. Gen. Jan. 4, 2005); Sager, *supra* note 333, at 534.

b. Expanding Counterterror Counterspeech

Some counterspeech efforts used to fight terror might be expanded to combat information warfare. The State Department's Global Engagement Center ("GEC") was established in April 2016, under Executive Order 13721.[366] The GEC's original mission was to track terrorist propaganda and disinformation, to develop consistent anti-terrorist messaging across government agencies, and to work with other governments and grassroots organizations to fight information warfare abroad.[367] The Center used social media to micro-target users vulnerable to radicalization.[368]

The 2017 National Defense Authorization Act ("NDAA") expanded GEC's mission to include countering the adverse effects of disinformation.[369] It also included a Privacy Act authorization for research and data analysis of foreign disinformation and communications.[370] In 2016 and 2017, Congress authorized the GEC to receive $120 million under the respective NDAAs to coordinate government-wide efforts to counter Russian and Chinese propaganda.[371] While the Center was underfunded during Rex Tillerson's tenure as Secretary of State, bipartisan backlash pushed funding to the GEC.[372] These funds have been dispersed to research disinformation tactics; support the counter-disinformation efforts of journalists, online influencers,

366 Exec. Order No. 13,721, 81 Fed. Reg.14,685 (Mar. 17, 2016).

367 Issie Lapowsky, *The State Department's Fumbled Fight Against Russian Propaganda*, WIRED (Nov. 22, 2017), https://www.wired.com/story/the-state-departments-fumbled-fight-against-russian-propaganda/.

368 *Id.*; *see also* Joby Warrick, *How A U.S. Team Uses Facebook, Guerrilla Marketing to Peel Off Potential ISIS Recruits*, WASH. POST (Feb. 6, 2017), https://www.washingtonpost.com/world/national-security/bait-and-flip-us-team-uses-facebook-guerrilla-marketing-to-peel-off-potential-isis-recruits/2017/02/03/431e19ba-e4e4-11e6-a547-5fb9411d332c_story.html (describing measures taken by the U.S. Government to use social media to combat extremism).

369 National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328, 130 Stat. 2546, § 1287 (2017).

370 *Id.* §1287(b)(10); *see also* Gardiner Harris, *State Dept. Was Granted $120 Million to Fight Russian Meddling. It Has Spent $0*, N.Y. TIMES (Mar. 4, 2018), https://www.nytimes.com/2018/03/04/world/europe/state-department-russia-global-engagement-center.html (describing the allocation of funds for fighting disinformation).

371 *See* Harris, *supra* note 370.

372 Robbier Gramer & Elias Groll, *State Department Ramps Up War Against Foreign Propaganda*, FOREIGN POLICY (Feb. 7, 2019), https://foreignpolicy.com/2019/02/07/with-new-appointment-state-department-ramps-up-war-against-foreign-propaganda/ (noting that Lea Gabrielle now heads the GEC); *see also* John S. McCain National Defense Authorization Act For Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018); Polyakova & Fried, *supra* note 4, at 8–9.

and fact-checkers; and develop new technology to combat disinformation.[373] The GEC's impact remains to be seen.

G. Regulating Online Platforms and Social Media

The Internet and social media platforms act as important fora for free speech and expression. Accordingly, any attempts to regulate online platforms and social media will raise First Amendment concerns, despite their status as private entities. Eric Posner goes so far as to assert that "any law that sought to blunt the force of Russian propaganda by controlling its distribution by Internet companies is unconstitutional."[374] He argues that because Supreme Court doctrine recognizes the right to receive information, free of government interference, censorship of Russian propaganda would not survive First Amendment scrutiny. However, Posner concludes by suggesting that the 2016 election demonstrates the drawbacks of an "unfettered 'marketplace of ideas.'"[375] Although the United States must respond to the danger of Russian and terrorist propaganda on social media, constitutional law serves as an obstacle. Despite the significant constitutional challenges involved, some government regulation of online platforms and social media may be permissible and appropriate to fight information warfare.

1. Hurdles to Regulating Online Platforms and Social Media

Some scholars have proposed making social media companies liable for illegal content posted by their users. David Howard, for example, has proposed holding information and social media companies responsible if their algorithms push false information for reasons of profit.[376] He also proposes fining social media companies for knowingly failing to remove illegal content.[377]

---

373 Polyakova & Fried, *supra* note 4, at 8–9.

374 Eric Posner, *Are Russian Trolls Protected by the First Amendment?*, ERIC POSNER (Feb. 17, 2018), http://ericposner.com/are-russian-trolls-protected-by-the-first-amendment/; *see also* Timmer, *supra* note 297, at 684 (noting that First Amendment protections for political speech and false speech make it difficult for a law targeting fake news to survive strict scrutiny).

375 Posner, *supra* note 374.

376 Howard, *supra* note 97, at 1375.

377 *Id.*

However, such proposals raise several major constitutional concerns. One concern is that requiring online platforms to be responsible for the content of their users' postings might qualify as collateral censorship. The more the U.S. Government is entangled with voluntary self-regulation of online platforms, the more the First Amendment becomes an issue. An online platform's behavior might constitute state action in certain circumstances, and therefore raise obligations under the First Amendment.[378] For example, in upholding online platform immunity under section 230 of the CDA,[379] the Ninth Circuit recognized the congressional purpose as partly to serve as free speech protection for users.[380] The court expressed concern with collateral censorship: if the government threatens to hold an online platform liable and the online platform then censors its users, the government would be partially responsible for limiting users' speech.[381]

Imposing an obligation on social media companies for illegal content posted by its users would be radical in the context of prior Supreme Court precedent protecting both true and false speech.[382] Few circumstances exist—and few should exist—in which the government is permitted to be the arbiter of what is true and what is false. If the government requires social media companies to do so on its behalf, that will violate the First Amendment. If social media companies operate independently to prohibit disinformation, the First Amendment is not implicated. However, if the government imposed some standard of care on online platforms to help combat disinformation, that would be a gray constitutional area. It could also be the beginning of a slippery slope with dangerous consequences for free speech. Technology companies tend to be risk-averse, especially if

---

378 *See* Klonick, *supra* note 94, at 1611 (questioning whether the *Packingham* decision opens the door for argument that social media platforms "perform quasi-municipal functions").

379 47 U.S.C. § 230 (2003).

380 Batzel v. Smith, 333 F.3d 1018, 1027-28 (9th Cir. 2003) (stating that the policy objectives are "(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation").

381 *Id.*; *see also* Klonick, *supra* note 94, at 1608 (discussing the *Zeran* court's concern of creating "collateral censorship" by holding Facebook liable for its users' speech).

382 *See, e.g.*, United States v. Alvarez, 567 U.S. 709 (2012) (plurality opinion) (ruling that the Stolen Valor Act was in violation of the First Amendment because it constituted a content-based restriction on free speech); N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (holding that damages cannot be awarded for defamatory falsehood unless actual malice is shown).

government sanctions are at play. Thus, holding social media companies liable for illegal content could lead to overbroad regulation or censorship of legitimate speech, especially political speech.[383]

Additionally, upon receiving notice of the potentially illegitimate speech, the company would have to engage in the resource-intensive inquiry as for whether or not the speech must be taken down. Censoring the speech would likely be less costly than being held liable, as not censoring allegedly illegal content may risk expensive litigation and adverse judgments.[384] The fear of "whether [the truth] can be proved in court or . . . the expense of having to do so" would encourage such collateral censorship.[385]

The spectrum of censorship arising from liability may range from mistakes to collateral censorship to even the prohibition of entire categories of speech on the site that produce higher risks of liability.[386] It could also lead to chilling speech by social media users, who currently operate in an environment where they can freely post anything and have it instantaneously shared around the world. If social media companies were to be held liable for their users' speech, users might hesitate to post or shrink away from using social media. Finally, such a policy could also undermine the concept that counterspeech is the primary solution to false speech, as advanced in *Sullivan* and *Alvarez*.

2. Avenues for Regulating Online Platforms and Social Media

Requiring online platforms to act as censors is constitutionally problematic for other reasons. Corporations, after all, have First Amendment rights of their own.[387] The government would not be able to compel social media companies to advance its own message or restrict the speech of users on its behalf.

---

383 BENKLER ET AL., *supra* note 20, at 362; Jamie Fly et al., *Fake News, Free Speech, and Foreign Influence: The Smart Way the U.S. Can Combat Disinformation*, HUMAN RIGHTS FIRST (Mar. 2018), https://www.humanrightsfirst.org/sites/default/files/Disinformation-Brief-March-2018.pdf.

384 Aaron Perzanowski, Comment, *Relative Access to Corrective Speech: A New Test for Requiring Actual Malice*, 94 CAL. L. REV. 833, 858 n.172 (2006) (arguing that "preserving free speech online requires costly investigation, legal analysis, and uncertain liability," if § 230 is read narrowly, which in turn suggests that "reasonable actors will immediately remove [flagged] speech without regard to the merits of the notification").

385 N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279 (1964).

386 Vulnerable, unpopular speech is most at risk here.

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

However, some regulations on online platforms might be feasible. Social media companies might be legally regulated as sellers of a customer service. Social media companies trumpet their ability to provide "community." In this sense, their services are much more akin to a gym or a café than to a media company. The governance of these companies over their communities can be likened to the regulation of a corporate restaurant chain or chain of gyms. Just like public accommodations can be regulated by the government to ensure that they do not violate the constitutional rights of those who are allowed inside, so too can social media. Just like the government can restrict who buys a gun, so too can the government restrict who is allowed on social media sites. And just like the government can police illegal activity in a private establishment, so too can it police illegal behavior on social media. While access to social media may be difficult to restrict post-*Packingham*, statutes narrowly tailored to advance a compelling state interest might be acceptable, so long as they do not burden more speech than necessary. *Packingham* also may not apply to the rights of non-U.S. persons or bots to access social media.

By regulating social media like other service providers, the government can solve some of the problems it has encountered in fighting information warfare. Social media companies could be held liable for allowing their platforms to be used for activities that undermine the integrity of the voting process since voting is a constitutional right and an act of expression. Any actions designed or motivated by the desire to suppress voter turnout would be of particular constitutional concern. Social media companies might be required to notify the government of such activities, although such a requirement could be construed as compelling speech by those companies. The government can also require that social media companies be held liable if they knew or should have had reason to know that a user was trying to disrupt elections on their sites. Narrowly tailored statutes targeted to the purpose of ensuring that social media users do not disrupt elections could allow the government to regulate social media constitutionally.

Social media companies could be required to conduct verification checks for all users who wish to join their sites to determine whether they are humans or bots. The government might also require users to regularly renew their verifications, perhaps randomly, and require repeated verifications for those who engage in behavior that suggests they are trying to disrupt elections. Social media companies could be held liable for failing to report bots who engage in activities disruptive to the electoral process.

Technology companies might also be required to notify their users and the U.S. Government that their sites are disseminating foreign propaganda.[388] Further, social media websites might also be required to disseminate information to their users about spotting and reporting fake news and posts designed to disrupt the U.S. electoral process. As discussed above, scholars have identified education campaigns about information warfare as an important part of the fight against it. Social media companies could be required to disseminate information to their users upon joining a social network and at regular intervals before and during electoral cycles. The government could require online platforms like Facebook and Google to provide specific information to its consumers to judge the materials posted.[389] If the online platform does not provide information, the online platform could be held liable for contempt or liable at a reckless standard. Even if Congress cannot legislate such a requirement, the government might ask social media companies to educate their users voluntarily. Reminding users of their important role in safeguarding the U.S. electoral process might generate a sense of online civic responsibility that would reinforce bonds within a social network, to which social media companies might subscribe. Facebook already regularly reminds its users to vote and to register to do so.

Other scholars have suggested additional useful tactics for responding to the Russian disinformation threat. Geltzer and Kupchan suggest adapting the framework of tracing and blocking terrorist financing to the current threat of information warfare.[390] They suggest legislation that would criminalize the acceptance of assistance from a foreign government that is aimed at influencing elections. For example, if a presidential candidate's campaign manager affirmatively responded to a Kremlin email offering to wage a disinformation campaign targeting his opponent in the 2020 election, that would constitute a criminal act. The goal would be to make social media companies and other sites more accountable, with a "know your source" requirement comparable to the "know your customer" requirement.[391] Howard argues that the government might also require online platforms to

388 *See* Geltzer & Kupchan, *supra* note 339 (suggesting requirement for source identification in social media).

389 However, social media companies like Facebook, Twitter, and Google "seem reticent to fully cooperate" and provide complete and usable data that will facilitate counter-disinformation efforts. Polyakova & Fried, *supra* note 4, at 14–15.

390 Geltzer & Kupchan, *supra* note 339.

391 *Id.*

modify their user agreements to limit disinformation, and to allow users to flag false or suspicious content.[392]

The ambiguous First Amendment status of online platforms and social media providers presents challenges for regulating them without chilling speech and trammeling on First Amendment rights. Legislation will be more likely to be constitutional if it puts the onus on users to safeguard their First Amendment rights, such as encouraging users to report suspected disinformation or requiring users to register bots. The more legislation puts the social media company in the position of a censor, the less likely it is to pass constitutional muster. Requiring a social media company to report suspicious behavior by its users presents a constitutional gray area, so legislation in this regard must be very narrowly tailored. Regulating online platforms as a category of service providers similar to other providers of places of communal gathering might show the most potential for preventing false speech designed to disrupt the electoral process.

3. "Voluntary" Actions by Online Platforms

Because regulation of online platforms and social media outlets presents constitutional difficulties, and because of the need for rapid action to protect voters against disinformation, some have proposed that online platforms voluntarily take steps to combat information warfare. Governments and the public have pushed social media platforms to voluntarily commit to actively policing their networks for fake news and disinformation, and to identify, label, and even suspend the botnets responsible for its creation and dissemination.

Online platforms have financial incentives to cooperate with governments that regulate their businesses. Voluntary compliance with government requests to help fight information warfare may help these companies avoid future regulation. Moreover, online platforms are accountable to their users and responsive to user demands and political pressures. Thus, online platforms have begun to take actions to combat

392 Howard, *supra* note 97, at 1375; *see also* Timmer, *supra* note 297, at 699–700 (describing a change implemented by Facebook whereby its users can flag content that may be fake).

information warfare. Political pressure[393] and social responsibility[394] have encouraged online platforms like Facebook, Twitter, and Google, to alter their platforms to combat fake news.[395]

Some commentators push for online platforms to serve as "de facto Internet police" because it is less costly and more efficient than for the government to do so.[396] They have called for online platforms to monitor subscriber conduct, remove risky subscribers from the network, report instances of computer crime on their sites, build constraints that automatically monitor and prevent illegal activity, and preserve data for law enforcement investigation.[397] However, all of these activities raise free speech concerns. If online platforms begin to act as Big Brother, users' speech will be chilled. Moreover, private companies tend to be risk-averse. As described earlier, online platforms may err in favor of over-censorship because of the difficulties in distinguishing protected from unprotected speech.[398]

The Federal Government could pressure online platforms to control the speech of their users through a "good corporate citizen" program, which requests online platforms to "voluntarily remove questionable content or alert government authorities to its existence."[399] Although the government lacks the legal authority to compel the removal of content, online platforms

---

393 *See, e.g.,* Cecelia Kang et al., *Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill*, N.Y. TIMES (Oct. 31, 2017), https://www.nytimes. com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html (reporting on social media executives appearing on capitol Hill to acknowledge their role in Russia's propaganda campaign).

394 *See, e.g.*, Mark Zuckerberg, FACEBOOK (Jan. 4, 2018, 10:40 AM), https://www.facebook.com/zuck/posts/10104380170714571 (discussing a "personal challenge" to focus on Facebook's role in "protecting our community from abuse and hate" and "defending against interference by nation states").

395 *See, e.g.*, Elizabeth Dwoskin, *Twitter Is Looking for Ways to Let Users Flag Fake News, Offensive Content*, WASH. POST (June 29, 2017, 3:16 PM), https://www.washingtonpost.com/news/the-switch/wp/2017/06/29/twitter-is-looking-for-ways-to-let-users-flag-fake-news; *How Google Fights Disinformation*, GOOGLE (Feb. 2019), https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/How_Google_Fights_Disinformation.pdf.

396 Chris Montgomery, Note, *Can* Brandenburg v. Ohio *Survive the Internet and the Age of Terrorism?: The Secret Weakening of a Venerable Doctrine*, 70 OHIO ST. L.J. 141, 165 (2009); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1095–96 (2001) (positing that "it may be more efficient for third parties to stop cybercrime from happening rather than to rely on prosecution").

397 *See Id.* at 1096–97 (outlining five strategies Internet Service Providers can use to combat fake news and other cybercrimes).

398 Montgomery, *supra* note 396, at 166.

399 *Id.* at 168.

may choose to remove content upon request instead of risking poor relations with the government. For example, under the CDA, online platforms are immune from civil liability for any "Good Samaritan" blocking or screening of "objectionable" material.[400]

Such actions by online platforms are complicated by the undefined legal status of online platforms, including social media websites, as media, service providers, and critical parts of the "new public square." Private companies ordinarily do not have First Amendment obligations toward their users. They certainly do not have a First Amendment burden to remove false and inciting speech. However, social media websites have more power to censor and impose restrictions on speech than many governments. Facebook can ban what it considers to be hate speech in its terms of service, but the U.S. Government cannot. Scholars have thus argued that self-censorship by social media companies causes First Amendment concerns. Some argue that social media platforms are a modern form of the press and, therefore, are generally protected by the First Amendment.[401] To do otherwise would contravene the First Amendment because it would inhibit legitimate democratic discourse.[402] Regardless of whether social media should be likened to the press, the public square, or something else entirely, the practice of censorship on social media "sits awkwardly" with traditional American values of open political debate and free expression.[403]

Moreover, as noted above, social media sites function as communities with quasi-governmental structures. They also provide important venues for free speech, expression, and discourse. Collateral censorship concerns may be raised if online platforms engage in a quasi-government function. A fine line may exist between censorship and voluntary action if the government puts strong pressure on online platforms to remove content against their will.

For these reasons, any voluntary actions by online platforms should also comport with First Amendment principles. Online platforms should

---

400 47 U.S.C. § 230(c)(2)(A)–(B) (2017).

401 Rachel E. VanLandingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism, and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1, 48 (2017) (making the case for protection from § 2339B, i.e., material support, criminal prosecution for allowing terrorists to post on their sites).

402 *Id.* (citing N.Y. Times Co. v. Sullivan, 376 U.S. 254, 278 (1964)).

403 Thomas H. Kean & Lee H. Hamilton, *Digital Counterterrorism: Fighting Jihadists Online*, BIPARTISAN POLICY CTR. 12 (Mar. 2018), https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-National-Security-Digital-Counterterrorism.pdf.

consider the primacy of political speech and the importance of political discourse on their platforms when considering any voluntary actions.

Rather than attempting to regulate the truth, technology companies might endeavor to identify "when 'news' sources are confined to a very narrow group of self-referring sources—a hallmark of disinformation—so that users are aware that [content] may be suspect."[404] Online platforms would not necessarily seek to suspend or censor the accounts, but act to alert their users about the dangers and warning signs of disinformation and radicalization. Clarifying the source of the material is in line with First Amendment principles as speaker identity can greatly impact trust factors, such as credibility, knowledge, motivation, and reliability.[405] Furthermore, foreign nations do not possess First Amendment interests, so "compelling the disclosure of their identity would not impose any speaker-side harms to offset the benefits of disclosure to listeners."[406]

One promising, data-driven tactic for countering divisive propaganda is Google's Jigsaw. This project, premised on counterspeech, was initially developed to thwart terrorist communications.[407] Jigsaw redirects YouTube users who search for radicalizing content toward persuasive, "user-created, de-radicalizing content."[408] The benefits of this approach are several-fold. First, consumers perceive online platform content as more authentic than U.S. Government messages.[409] Second, the data-driven approach can better identify hidden, counter-argument content[410] that resembles propaganda but was not designed to do so directly. Examples might include citizen journalism and documentaries and content featuring religious figures who refute extremist narratives.[411] Third, these approaches do not depend on the government's ability to apply regional, linguistic, cultural, or religious

404 Robert D. Blackwill & Philip H. Gordon, *Containing Russia, Again: An Adversary Attacked the United States—It's Time to Respond*, COUNCIL ON FOREIGN REL. (Jan. 19, 2018), https://www.cfr.org/article/containing-russia-again-adversary-attacked-united-states-its-time-respond.

405 Helen Norton, *(At Least) Thirteen Ways of Looking at Election Lies*, 71 OKLA. L. REV. 117, 124 n.31 (2018) ("[L]isteners often use the speaker's identity as a proxy for the message's quality and credibility.").

406 Thai, *supra* note 68, at 318.

407 Kean & Hamilton, *supra* note 403, at 22.

408 *Id.*

409 *Id.*

410 *See* THE REDIRECT METHOD, A BLUEPRINT FOR BYPASSING EXTREMISM 5 (last accessed Oct. 23, 2019), https://redirectmethod.org/downloads/RedirectMethod-FullMethod-PDF.pdf.

411 *Id.* at 6.

expertise to determine the credibility of messages. Instead, real-world user behavior can be used to determine which messages are persuasive at radicalization or counter-radicalization.[412] Other data-driven projects, such as those run by Graphika, Oxford University's Computational Propaganda Project, the Atlantic Council's Digital Forensic Research Lab, YouTube's AlgoTransparency, and Public Editor, are helpful in tracking and exposing disinformation that social media companies can remove.[413]

Flagging and the voluntary removal of content as an avenue to counter propaganda may be more coercive to users than countermessaging or redirection, but would better conform to First Amendment requirements and be more palatable to the companies' user bases.[414] However, social media companies run a similar credibility risk to that faced by the government. Social media corporations' use of their users' data and psychological profiling has caused many traditional media outlets, researchers, and users to view their editorial interventions with skepticism.[415]

Another solution that social media companies are currently trying is signaling source quality. Facebook, for example, has begun to surface fact-checked articles next to disputed ones,[416] add "trust indicators" to include information about the publication, corrections, and ethics policies,[417] and crowdsourced the trust rankings of news sources to its userbase.[418] Some social media sites have also excluded bot activity from measures of "trending" content.[419] Platforms have also tried limiting bots and "cyborgs" from spreading news.[420] Although malign actors may be able to design countermeasures to these efforts, social media companies will have incentives

412 Kean & Hamilton, *supra* note 403, at 22.

413 Polyakova & Fried, *supra* note 4, at 15.

414 Kean & Hamilton, *supra* note 403, at 23.

415 *See id.*

416 *See, e.g.*, Jeff Smith et al., *Designing Against Misinformation: Facebook Design*, MEDIUM (Dec. 20, 2017), https://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2.

417 Casey Newton, *Facebook Adds Trust Indicators to News Articles in an Effort to Identify Real Journalism*, VERGE (Nov. 16, 2017), https://www.theverge.com/2017/11/16/16658538/facebook-trust-indicators-fake-news-trust-project.

418 Elizabeth Dwoskin & Hamza Shaban, *Facebook Will Now Ask Users to Rank News Organizations They Trust*, WASH. POST (Jan. 19, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/19/facebook-will-now-ask-its-users-to-rank-news-organizations-they-trust/.

419 Lazer et al., *supra* note 27, at 1096.

420 *Id.* at 1096. Lazer et al. define cyborgs as "users who automatically share news from a set of sources, with or without reading them." *Id.*

to keep combatting them if users value the credibility of their chosen platforms. These are positive steps, but more research is needed to evaluate their effectiveness.

The government can carefully pressure social media companies to provide an editorial function in regulating what is allowed on the sites, although these actions raise a concern of censorship. The government employed such tactics in combatting foreign terrorist groups. The DOJ's Cyber Digital Task Force Report foresees the FBI assisting in providers' voluntary efforts to identify and combat malign foreign influence operations, just as it has in addressing terrorist use of social media.[421] Upon government request, in many of their "Terms of Service," online platforms explicitly prohibit posts promoting violent or terrorist acts. The government has pressured social media companies to police their users' accounts for terrorist-related activity.[422] Social media companies have thus taken some editorial control via terms of service or user agreements that allow them to remove posts or delete accounts of terrorists or their supporters.[423] Some corporations, like Twitter, have suspended or blocked hundreds of thousands of terrorist accounts—often before their first post.[424] Suspending pro-extremist social media accounts does not appear to sufficiently prevent new, pro-extremist group accounts from sprouting up.[425] But, although the terrorists may quickly recreate the accounts, these "returning accounts" do not regain their previous level of traction. From February 2016 to March 2017, there was a dramatic decline of 76% in the number of tweets from English-language Islamic State sympathizers "from the most active to the least active week."[426] The policy of suspending accounts, however, may have other problems. Beyond free speech issues and the loss of intelligence

421 CYBER DIGITAL TASK FORCE REPORT, *supra* note 6, at 7.

422 VanLandingham, *supra* note 401, at 16.

423 *Id.* at 17; *see also* Klein & Wueller, *supra* note 298, at 10 (noting that "many Internet advertising companies have updated their program policies to deny services to fake news publishers").

424 Kean & Hamilton, *supra* note 403, at 11. Twitter also removed almost 4800 accounts spreading disinformation that were linked to the Iranian Government in their efforts to prevent election interference. *See* Kari Paul, *Twitter Removes Thousands of Accounts Linked to Iran Government*, GUARDIAN (June 13, 2019, 3:08 PM), https://www.theguardian.com/technology/2019/jun/13/twitter-iran-accounts-deleted-iranian-government-election-interference.

425 Ariel V. Lieberman, Note, *Terrorism, the Internet, and Propaganda: A Deadly Combination*, 9 J. NAT'L SECURITY L. & POL'Y 95, 102 (2017).

426 Audrey Alexander, *Digital Decay: Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, GEO. WASH. U. PROGRAM ON EXTREMISM 7, 15 (Oct. 2017), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.

gathering opportunities, suspensions may cause further radicalization by pushing extremists into insular online communities without moderate voices.

Similar efforts by online platforms, whether coerced or voluntary, might be useful in combatting information warfare. However, they make the online platform, not the consumer of information, the arbiter of truth. Although such actions may not violate First Amendment freedoms, they raise concerns about chilling speech and censorship that run contrary to First Amendment ideals.

4. The Utility of Self-Regulation?

As a tool for combatting information warfare, voluntary self-regulation by online platforms has many inherent flaws. Online platforms' efforts to remove posts or cooperate are likely to be inconsistent.[427] Voluntary self-regulation depends on the willingness of those at the helm of a social media company at any given time to comply. New social media companies sprout up rapidly, making it difficult for the government to work with all of them. Smaller companies may not have the capacity to monitor users' accounts closely. Self-regulation also raises the problem of the proverbial fox guarding the henhouse. Social media companies have every incentive to look like they are cooperating with the government while plausibly claiming deniability when their users misbehave. Private companies do not provide U.S. persons with the same procedural safeguards and transparency as the government would require for infringement on speech.[428] Encouraging companies to censor content without any form of due process removes transparency and could chill speech.

More research is needed to determine the conditions under which voluntary self-regulation by online platforms and their users can fight information warfare. For example, a recent study reported in the *New York Times* revealed that most users were unable to distinguish Russian fake news postings from real political advertisements, although trained online platform and social media employees might do better.[429] Government guidelines for

427 Michelle Roter, Note, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1394 (2017); BENKLER ET AL., *supra* note 20, at 365 (discussing different approaches by social media companies to regulate speech).

428 Roter, *supra* note 427, at 1381.

429 Keith Collins & Sheera Frenkel, *Can You Spot the Deceptive Facebook Post?*, N.Y. TIMES (Sept. 4, 2018), https://www.nytimes.com/interactive/2018/09/04/technology/facebook-influence-campaigns-quiz.html.

good corporate citizenship by social media companies and their users would be a good start to combatting information warfare but would be insufficient on their own.

CONCLUSION

The First Amendment protects the most hallowed of American freedoms. However, information warfare has weaponized free speech against us. Adversaries of the United States have taken advantage of our prized freedom of speech and used it to undermine our electoral process, the very foundation of democracy itself. To fight against information warfare, the U.S. Government is faced with a paradox: while our enemies enjoy and exploit our citizens' right to free speech, Congress may need to restrict the freedom of speech of Americans to fight our enemies' speech. Congress and administrative agencies must tread carefully to avoid unduly restricting First Amendment freedoms in the name of national security. Allowing our adversaries to enjoy First Amendment freedoms—while Americans truly cannot—would help our enemies win.

Faced with the enormous challenge of balancing the First Amendment with national security concerns, the United States has passed little legislation and issued few regulations to fight information warfare, especially as related to elections. Several bills to enhance U.S. Government efforts to combat information warfare are currently stalled in Congress, in part due to concerns about their lack of adequate procedural and constitutional safeguards.[430] Meanwhile, the threat increases, as Russia continues its information warfare campaigns with unparalleled speed. Russia, Iran, North Korea, and China are continuing to develop information warfare programs. U.S. inaction to combat them will likely encourage other foreign governments to engage in similar influence operations.

---

430 *See, e.g.*, Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019); Defending American Security from Kremlin Aggression Act of 2019, S. 482, 116th Cong. (2019); Defending Elections from Threats by Establishing Redlines Act of 2018, H.R. 4884, 115th Cong. (2018); Countering Foreign Propaganda Act of 2018, H.R. 5354, 115th Cong. (2018); Foreign Agents Registration Amendments Act of 2018, S. 2482, 115th Cong. (2018); REFUSE Act, H.R. 6249, 115th Cong. (2018); Disclosing Foreign Influence Act, S. 2039, H.R. 4170, 115th Cong. (2017); Foreign Agent Lobbying Transparency Enforcement Act, S. 1679, 115th Cong. (2017); Foreign Agents Registration Modernization and Enforcement Act, S. 625, 115th Cong. (2017); Foreign Agents Registration Modernization and Enforcement Act, H.R. 2811, 115th Cong. (2017); Honest Ads Act, S. 1989, 115th Cong. (2017); Ethics in Foreign Lobbying Act of 2016, H.R. 6057, 114th Cong. (2016).

This Article outlines what must be done to reform U.S. laws to fight information warfare. A whole-of-government approach, involving the Departments of State, Defense, and Justice, the military, the intelligence community, and other civilian agencies, is necessary to fight it. The work of these agencies is governed by a patchwork of laws that needs to be reformed, synthesized, and harmonized with the United States' commitment to free speech and other civil liberties. Legal reconceptions of First Amendment doctrine, privacy, and the role of the Internet and social media in society are necessary to combat information warfare effectively.

This Article's analysis of U.S. laws governing information warfare presents implications for how the U.S. military may conduct information operations abroad. Military information and cyber operations are covered by a separate and overlapping legal framework than that discussed above, reflecting the differing requirements of kinetic warfare, other operations abroad, the law of armed conflict, international law, and sometimes covert operations. However, military operations must conform to constitutional principles and many other domestic laws and policies of the United States. Even though military operations are within the purview of the Executive Branch, their constitutional validity may rest on congressional approval or limitations. The court of public opinion, which is increasingly important in military operations, is also concerned with constitutional liberties.

Furthermore, military information operations may produce collateral effects that affect U.S. nationals and involve the functioning of online platforms, especially if they are subject to a cyber intrusion.[431] Perhaps most importantly, military operations increasingly rely on a whole-of-government approach, in which the military works closely with other government agencies to coordinate a unified fight against a foreign adversary. Thus, the analysis above may be useful to the DOD in planning future military efforts to fight information warfare.

The information warfare threat leads to a clash between two values that are fundamental to American society: freedom of speech and free-and-fair elections. Both ideals are grounded in the First Amendment, which has traditionally protected political speech above all forms of expression. The

---

431 The Pentagon has empowered the U.S. Cyber Command to take offensive cyberaction that may be used to counter aggressive foreign disinformation campaigns. *See* David E. Sanger, *Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict*, N.Y. TIMES (June 17, 2018), https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html.

environment in which political speech is made and received is vastly different from the original Millian conception of the marketplace of ideas. So much speech now floods the marketplace that little can be heard at all. Some speakers can shout more loudly and rapidly than others due to mechanization. Shopper-listeners lock themselves in echo chambers alongside only customers of similar views. The flood of so much information into the marketplace at once, plus the poor acoustic conditions, make it difficult for true speech to be heard over falsities.

In this new speech environment, courts should be more concerned with the validity and intent of political speech than the availability of that speech. Deciding what speech is and what speech is not "political" is dangerous territory for the government. Instead, legislators and courts should take a narrower approach, focusing on speech made by foreign individuals and foreign agents in the electoral context. They can also act to protect the fundamental constitutional right to vote and the electoral process that surrounds it. Just as importantly, courts can recognize social media companies for the unique entities that they are: part press, part service provider, and part corporate governance entity. Legislators may also regulate social media companies accordingly.

Besides intelligence collection, more academic research on information warfare is desperately needed to make the combat effort effective. Research is needed to understand the nature of information warfare, to predict how it will develop, and to develop countertactics and operations accordingly. Fourth Amendment concerns with protecting Americans against unreasonable search and seizure must also be fully explored. Experiments are needed to determine what tactics will work to fight information warfare, and under which conditions. Research is also necessary to determine who is susceptible to information warfare. Academics, government, and social media providers must cooperate to achieve a holistic picture of the information battlefield. Further research is critical to assess the impact of disinformation campaigns on U.S. elections. Without clarifying the extent or nature of the harm caused by disinformation campaigns, government agencies may find it difficult to attract resources or develop effective programs to combat the threat.

Disinformation threatens the existence of a well-informed public, and therefore, democracy itself. As Justice Robert Jackson aptly noted, the

Constitution should not be "a suicide pact."[432] Likewise, the United States should not fall on the First Amendment's double-edged sword. The time has come for courts to reaffirm the primacy of political speech by protecting it from foreign information operations. Nothing less than the meaning of the First Amendment, the right to privacy, and the foundations of American democracy are at stake.

---

432 Terminiello v. City of Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting).