

FARA ON FACEBOOK: MODERNIZING THE FOREIGN AGENTS REGISTRATION ACT TO ADDRESS PROPAGANDISTS ON SOCIAL MEDIA

*Joshua R. Fattal**

In court filings in 2018, Special Counsel Robert S. Mueller III claimed that Russian social media disinformation actors during and after the 2016 election did not fulfill their obligation to register as agents of a foreign principal under the Foreign Agents Registration Act (“FARA”), the primary federal law concerning the political activities of foreign entities in the United States. As of this Article’s writing, no comprehensive study has been undertaken to evaluate how FARA’s statutory terms may apply to foreign propagandists who seek to influence U.S. political opinion primarily through disinformation campaigns on social media. This Article aims to fill this gap in the growing literature on this subject.

The Article begins by recounting the origins of FARA and telling the story of its uses up to the present day. The Article then describes the advent of disinformation on social media, focusing on the alleged Russian disinformation activity that began before the 2016 U.S. presidential election and that has continued in some shape or form until today. Next, the Article tackles some of the novel statutory interpretation issues and enforcement questions that arise when applying FARA’s terms to social media disinformation actors: Do the terms of the law retain significance when both the agent and the foreign principal are operating on foreign soil? What foreign propaganda materials should the Department of Justice require to be labeled under FARA, if any? What might a compliance regime look like in the context of foreign propagandists who reside outside of U.S. jurisdiction? The Article will attempt to put forth some possible answers to these questions, focusing on both the challenges that arise with registering disinformation actors on social media and the opportunities that may present themselves for tackling this threat.

* Joshua R. Fattal received his J.D. from the New York University School of Law in 2018 and is currently an attorney-advisor in the Office of the General Counsel at the U.S. Department of Homeland Security. This Article was written and accepted prior to the start of the author’s current position, and the views expressed here are his own and do not necessarily reflect the views and opinions of DHS, the U.S. government, or any other former employer. The author would like to thank Professors Bob Bauer, Randy Milch, and Jason Schultz for their generous guidance and mentorship throughout the writing process, and Brooke Gottlieb and the Journal’s staff for their editorial work. All errors are the author’s alone.

INTRODUCTION	904	R
I. THE FOREIGN AGENTS REGISTRATION ACT	908	R
A. History and Focus of the Act	908	R
B. FARA’s Recent Resurgence	913	R
II. FOREIGN ORGANIZED DISINFORMATION CAMPAIGNS DURING AND AFTER 2016	916	R
III. MODERNIZING THE FOREIGN AGENTS REGISTRATION ACT	923	R
A. The Agent and Foreign Principal Relationship in the Social Media Context	924	R
B. Attribution in the Social Media Context	929	R
C. Excluding U.S. Persons from FARA Registration .	933	R
D. Social Media Posts as Informational Materials	934	R
E. Enforcing FARA in the Digital Age	938	R
F. Policy Considerations for the Tech Community ...	944	R
CONCLUSION	946	R

INTRODUCTION

In February 2018, Special Counsel Robert S. Mueller III brought charges against thirteen Russian individuals and three organizations allegedly involved in a coordinated disinformation campaign aimed at the 2016 United States political process.¹ One of the laws that the special counsel claimed these Russian actors violated is the Foreign Agents Registration Act (“FARA” or “Act”).² FARA, the central law governing the activities of agents of foreign entities that act in the United States, was enacted in 1938, a time in which Nazi propaganda took place out in the open on American soil. Since then, FARA has been used most often to register lobbyists and other political actors within the United States. The special counsel’s court filings notably

1. An additional complaint from September 29, 2018, against other members of this alleged conspiracy was unsealed on October 19, 2018. See 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-mid-terms-edition>. While this Article will take the facts in these indictments as true, this Article takes no position on the effectiveness of these kinds of disinformation campaigns when it comes to influencing an election or any other political results and recognizes the difficulty in making that kind of determination. See, e.g., Benedict Carey, ‘Fake News’: *Wide Reach but Little Impact, Study Suggests*, N.Y. TIMES (Jan. 2, 2018), <https://www.nytimes.com/2018/01/02/health/fake-news-conservative-liberal.html>. This Article therefore uses the phrase “2016 U.S. political process” to indicate that the disinformation campaign discussed here did not necessarily have any impact on the 2016 U.S. political elections.

2. See Indictment ¶ 7, *United States v. Concord Mgmt. & Consulting LLC*, 347 F. Supp. 3d 38 (D.D.C. 2018) (No. 1:18-cr-00032-DLF), 2018 WL 914777 [hereinafter Indictment].

used FARA to target propaganda that is disseminated not on U.S. streets or in government offices, but by foreigners on social media. These propagandists, unlike those at the time of FARA's enactment, are anonymous, covertly working to influence U.S. political opinion from abroad.

The use of FARA in the context of foreign actors on social media is unprecedented. As the attorney for one of the indicted Russian organizations put it: “[N]ever before has a foreign corporation . . . with no presence in the United States, been charged criminally for . . . the political speech of individuals on social media, at rallies, or in advertisements during a U.S. presidential election campaign.”³ Similarly, in the words of a former head of the FARA Unit of the Department of Justice (“DOJ”): “[T]his case may represent the first time the DOJ has charged foreign nationals, operating predominantly from a foreign country, with criminal violations of FARA”⁴

Despite the vast differences between propagandists in the 1940s and today's social media propagandists, and the fact that FARA has never before been used in the social media context, little analysis has been done regarding whether, and how, FARA's statutory terms might apply to foreign online disinformation actors.⁵ Perhaps this is the reason why DOJ's FARA Unit has not yet actively registered any foreign disinformation actors: a ‘Quick Search’ on the DOJ FARA page for active foreign registrants located in Russia returns only seven results, none of them actors on social media—a surprisingly low number given all the reports of social media propagandists traced back to Russia in the last few years.⁶

3. See Kevin Poulsen & Spencer Ackerman, *The Most Shocking Moments of the New Russia Complaint, from ‘Civil War’ to ‘Fake’ Rubio to ‘Colored LGBT,’* DAILY BEAST (Oct. 19, 2018, 4:31 PM), <https://www.thedailybeast.com/the-most-shocking-moments-of-the-new-russia-indictment-from-civil-war-to-fake-rubio-to-colored-lgbt>.

4. David Laufman, *FARA Enforcement: The Year Ahead*, LAW360 (Feb. 7, 2019, 2:06 PM), <https://www.law360.com/articles/1126502/fara-enforcement-the-year-ahead>.

5. Rather than focusing on FARA, legislative attempts to respond to disinformation campaigns on social media have so far focused on the Honest Ads Act, a bill that, if enacted, would require social media companies to disclose who is buying political advertisements on their platforms. See David Kravets, *Proposed Law Would Regulate Online Ads to Hinder Russian Election Influence*, ARS TECHNICA (Oct. 23, 2017, 11:24 AM), <https://arstechnica.com/tech-policy/2017/10/proposed-law-would-regulate-online-ads-to-hinder-russian-election-influence/>.

6. See *FARA Quick Search of Active Registrants for all Countries/Location*, U.S. DEP'T OF JUSTICE, https://efile.fara.gov/pls/apex/f?p=185:11:0::NO:RP,11:P11_DATERANGE,P11_FROMDATE,P11_TODATE:N,05%2F04%2F2019,05%2F04%2F2019 (last visited May 4, 2019).

As of this Article's writing, FARA itself has also never been found to directly apply to foreign social media actors. The special counsel's indictment asserts that the Russian defendants failed to register as foreign agents carrying out political activities within the United States, but it charges the defendants with the crime of conspiracy to defraud the United States under 18 U.S.C. § 371, not with violating FARA itself.⁷ The crime of conspiracy does not need to be connected to a specific underlying crime, such as a FARA violation.⁸ However, in a court order, a U.S. district judge suggested that "the government may ultimately have to prove that the defendants agreed to a course of conduct that, if carried out, would [fall under FARA's statutory requirements and] require disclosure to the . . . DOJ."⁹ In other words, it may at some point become important to determine whether the conduct of these social media actors falls under FARA itself, but no analysis has yet been done to determine how the statute would apply in such a case. This Article therefore seeks to study what a FARA registration requirement for social media disinformation actors might look like.

Though the most high profile example of foreign disinformation on social media—Russian interference in the 2016 U.S. political process—has come and gone, social media disinformation campaigns by foreign actors have continued to the present day. A study published in October 2018, for example, found that more than eighty percent of the Twitter accounts that frequently shared links to phony news reports during the 2016 election process remained active two years later.¹⁰ While reports indicate that Russia did not interfere in the 2018 election cycle to the extent that it has been reported to have interfered in the 2016 cycle,¹¹ Russia continued to use social media and fake personas to influence positions on opposite ideological sides with the aim

7. Emma Kohse & Benjamin Wittes, *About that Russia Indictment: Robert Mueller's Legal Theory and Where It Takes Him Next*, LAWFARE (Mar. 7, 2018, 7:00 AM), <https://www.lawfareblog.com/about-russia-indictment-robert-muellers-legal-theory-and-where-it-takes-him-next>.

8. *See id.*

9. *United States v. Concord Mgmt. & Consulting LLC*, 347 F. Supp. 3d 38, 51 (D.D.C. 2018).

10. Craig Timberg, *Fake-News Ecosystem Still Thrives, Two Years After the 2016 Election, New Report Says*, WASH. POST (Oct. 4, 2018), <https://www.washingtonpost.com/technology/2018/10/04/fake-news-ecosystem-still-thrives-two-years-after-election-new-report-says/> (citing MATTHEW HINDMAN & VLAD BARASH, KNIGHT FOUND., DISINFORMATION, 'FAKE NEWS' AND INFLUENCE CAMPAIGNS ON TWITTER (2018), https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/238/original/KF-DisinformationReport-final2.pdf).

11. Kevin Poulsen & Spencer Ackerman, *Researchers: No Evidence That Russia is Messing with Campaign 2018—Yet*, DAILY BEAST (Oct. 8, 2018, 8:01 PM), <https://>

of further polarizing the United States.¹² Social media companies have consistently identified new influence campaigns from other countries, including Iran, that mimic Russia's techniques and are aimed at misleading people around the world.¹³ As such, it is highly likely that foreign countries and other foreign entities will continue to seek to influence U.S. political opinion using social media in one way or another during the coming years. It is therefore critical to contemplate the ways to effectively respond, considering the wide range of tools at both technology companies' and the U.S. government's disposal.

Part I of this Article familiarizes the reader with FARA's history up until the present day. Section I.A explores the earlier versions of the Act, from 1938, 1942, and 1966, and studies the legislative history surrounding each version to illuminate the original goals for the Act's passage and the ways it has been used since. Section I.B then details some of the ways in which FARA has made headlines in recent years, in particular its increasing importance to foreign lobbyist registration. Part II briefly summarizes the kind of social media-based disinformation campaign that this Article is concerned about, using the online activity that began before the 2016 presidential election as its focus.

Part III then applies the law as identified in Part I to the facts as identified in Part II. Section III.A begins by recognizing and resolving some of the statutory issues that arise when attempting to apply FARA to social media actors. Section III.B takes a closer look at who the operatives involved in a social media campaign are and considers whether it is possible to attribute posts to particular actors with any degree of certainty. Section III.C discusses a category of actors DOJ should ensure do not get caught in FARA's orbit: U.S. persons unwittingly involved in these online campaigns. Section III.D studies how FARA's labeling requirements could apply to social media postings. Section III.E considers how the registration and labeling requirements of the Act may be enforced practically to tackle the social media prob-

www.thedailybeast.com/researchers-no-evidence-that-russia-is-messing-with-campaign-2018yet.

12. See Julian E. Barnes, *Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says*, N.Y. TIMES (Dec. 21, 2018), <https://www.nytimes.com/2018/12/21/us/politics/russia-midterm-election-influence-coates.html>.

13. Sheera Frenkel & Nicholas Fandos, *Facebook Identifies New Influence Operations Spanning Globe*, N.Y. TIMES (Aug. 21, 2018), <https://www.nytimes.com/2018/08/21/technology/facebook-political-influence-midterms.html>; see also Sheera Frenkel et. al, *Russia's Playbook for Social Media Disinformation Has Gone Global*, N.Y. TIMES (Jan. 31, 2019), <https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html> (discussing how Bangladesh and Venezuela are among the other countries that have used social media to disseminate government talking points).

lem. Section III.F discusses some broader policy ideas concerning the proposals discussed in the prior two sections. Finally, the Conclusion discusses the challenges that lie ahead.

I.

THE FOREIGN AGENTS REGISTRATION ACT

The Foreign Agents Registration Act is the central law governing the activities of agents of foreign entities acting in the United States.¹⁴ The Act generally requires that “agents of foreign principals” who undertake certain activities on behalf of foreign interests—including engaging within the United States in political activities for, or in the interests of, such foreign principals—register with DOJ, file copies of “informational materials” that they distribute,¹⁵ and maintain records of their activities.¹⁶

A. *History and Focus of the Act*

FARA was originally enacted in 1938,¹⁷ and was designed to promote transparency with regards to foreign propaganda.¹⁸ The Act was inspired by the global political dynamics of the 1930s. In 1935, the U.S. House of Representatives convened the McCormack Committee (the first House Un-American Activities Committee) to investigate the existence and effects of Nazi propaganda efforts in the United States, as well as the use of “subversive propaganda” distributed by other foreign countries more generally.¹⁹ The spread of fascism, com-

14. 22 U.S.C. §§ 611–621 (2012). Section 611 defines “foreign principal” as the government or political party of a foreign country, a person domiciled abroad, or any foreign “partnership, association, corporation, organization, or other combinations of persons.”

15. *Id.* § 614(a).

16. *Id.* § 615.

17. Foreign Agents Registration Act, Pub. L. No. 75-583, 52 Stat. 631 (1938) (codified at 22 U.S.C. §§ 611–621 (2012)).

18. See CYNTHIA BROWN, CONG. RESEARCH SERV., R45037, THE FOREIGN AGENTS REGISTRATION ACT (FARA): A LEGAL OVERVIEW 1 (2017), <https://fas.org/sgp/crs/misc/R45037.pdf> (citing *Viereck v. United States*, 318 U.S. 236, 241 (1943)) (“The general purpose of the [Act of 1938] was to identify agents of foreign principals who might engage in subversive acts or in spreading foreign propaganda, and to require them to make public record of the nature of their employment.”). *But see Attorneys Under the Foreign Agents Registration Act of 1938*, 78 HARV. L. REV. 619, 620 (1965) (arguing that the legislative history and high penalties of the original Act suggest that it was designed more to curb subversive and marginally subversive activities than to provide the public with information about foreign agency relationships).

19. See H.R. REP. NO. 74-153, at 1 (1935). “The National Socialist German Labor Party, through its various agencies, furnished tons of propaganda literature, which in most cases was smuggled into this country. Some of it, however, came through our Customs, because there is no law against it.” *Id.* at 6. The investigation into “subver-

munism, and economic unrest during the interwar period drove Congress's concern that foreign sources would seek to influence the American people and government.²⁰ The House Report of the Seventy-Fifth Congress declared that the basic purpose of the Act was to focus a "spotlight of pitiless publicity" on organizations that are financed by "foreign governments or foreign political groups" in order to spread propaganda and "influence the external and internal policies of this country."²¹ As the House Judiciary Committee described in its recommendation to adopt the legislation:

Incontrovertible evidence has been submitted to prove that there are many persons in the United States representing foreign governments or foreign political groups, who are supplied by such foreign agencies with funds and other materials to foster un-American activities, and to influence the external and internal policies of this country, thereby violating both the letter and the spirit of international law, as well as the democratic basis of our own American institutions of government.²²

The Judiciary Committee further noted that this interference was often hard to identify: "Evidence before the Special Committee on Un-American Activities disclosed that many of the payments for this propaganda service were made in cash by the consul of a foreign nation, clearly giving an unmistakable inference that the work done was of such a nature as not to stand careful scrutiny."²³ The House Judiciary Committee therefore recommended:

Congress should enact a statute requiring all publicity, propaganda, or public-relations agents or other agents or agencies, who represent in this country any foreign government or a foreign political party or foreign industrial or commercial organization, to register with the Secretary of State of the United States, and to state name and location of such foreign employer, the character of the service rendered, and the amount of compensation paid or to be paid therefor.²⁴

sive propaganda" was interpreted to include fascist and communist activities as well. *Id.* at 9, 12; *see also* *Viereck v. United States*, 318 U.S. 236, 241 (1943) (discussing the need during the "critical period before the outbreak of the war" to identify agents of foreign principals "who might engage in subversive acts or in spreading foreign propaganda").

20. H.R. REP. NO. 74-153, at 2.

21. Attorney Gen. of U.S. v. *Irish People, Inc.*, 684 F.2d 928, 939 (D.C. Cir. 1982) (quoting H.R. REP. NO. 75-1381, at 1-2 (1937)).

22. H.R. REP. NO. 75-1381, at 1-2 (1937).

23. *Id.* at 2.

24. H.R. REP. NO. 74-153, at 23.

The attack on Pearl Harbor spurred Congress to amend and extend the 1938 Act.²⁵ The amended language sought to more clearly attribute the sources of materials disseminated by agents of foreign powers, and expressly declared that the Act's policy and purpose is to protect "the national defense, internal security, and foreign relations of the United States."²⁶ The amendment also contained a definition of "political propaganda,"²⁷ which has since been stricken from the Act,²⁸ and introduced a labeling requirement, requiring all registrants to mark "political propaganda" with a source-disclosure statement.²⁹

From its passage in 1938 until 1966, FARA focused primarily on traditional political propagandists. But the 1966 amendments, which form the core of the current Act,³⁰ shifted the Act's focus to protecting the integrity of the government's decision-making process.³¹ This shift was due largely to the changing nature of foreign influence: attention in the 1960s focused more on increasingly varied and sophisticated

25. See *Attorney Gen. of U.S.*, 684 F.2d at 939 (citing S. REP. NO. 77-913 (1941)).

26. Act of Apr. 29, 1942, ch. 263, 56 Stat. 248; see also *Attorney Gen. of U.S.*, 684 F.2d at 937 ("It should also be obvious—and reviewing the legislative history amply confirms this—that to the extent FARA focuses on subversion by foreign powers, foreign policy concerns become inevitable. The Attorney General may channel his limited resources against agents of those powers inimical to the United States, who are more likely to subvert our allies and interest.").

27. "Political propaganda" is:

[A]ny 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.

56 Stat. at 250–51 (repealed 1995).

28. See Lobbying Disclosure Act of 1995, Pub. L. No. 104-65, § 9, 109 Stat. 691, 699.

29. See Act of Apr. 28, 1942, ch. 263, 56 Stat. 248, 255 (codified at 22 U.S.C. § 614(b) (2012)); *Keene v. Meese*, 619 F. Supp. 1111, 1115 (E.D. Cal. 1985), *rev'd*, 481 U.S. 465 (1987).

30. See *Attorney Gen. of U.S.*, 684 F.2d at 941.

31. See OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, AUDIT OF THE NATIONAL SECURITY DIVISIONS' ENFORCEMENT AND ADMINISTRATION OF THE FOREIGN AGENTS REGISTRATION ACT 2 (2016).

kinds of subversive activities.³² With the Axis Powers defeated, and the existence of new federal legislation, such as the Smith Act, aimed directly at agents seeking to violently overthrow the government, FARA was no longer needed to regulate subversive activity.³³ As such, the Act gradually refocused from its original emphasis on subversive activity to an emphasis on protecting government decision-making from foreign influence.³⁴ These amendments had the practical effect, according to DOJ's FARA Unit staff, of reducing the incidence of criminal FARA prosecutions in favor of increased civil and administrative resolution of FARA violations.³⁵ The "cornerstone" of the Registration Unit's enforcement efforts had become "encouraging voluntary compliance."³⁶

Congress again amended FARA in 1995 as part of a broader effort to reform lobbying disclosure laws, known as the Lobbying Disclosure Act (LDA).³⁷ These amendments limited FARA's registration requirements to agents of foreign governments and foreign political parties, allowing agents of other foreign entities, such as foreign companies, to register under the LDA's disclosure requirements.³⁸ The 1995 amendments also removed the term "political propaganda" from FARA, replacing it with the undefined term "informational materials."³⁹ DOJ reports that this change occurred because Congress believed that the term "propaganda" was an unnecessary remnant of the original law, and found that the phrase "informational materials" better reflected the shift in the Act's focus towards public disclosure of agents engaged in the U.S. political process.⁴⁰

32. See David L. Simiele, *Disclosure Under the Foreign Agents Registration Act of 1938, as Amended*, 14 WES. RES. L. REV. 579, 584 (1963) (citing STAFF OF S. COMM. ON FOREIGN RELATIONS, 87TH CONG., NONDIPLOMATIC ACTIVITIES OF REPRESENTATIVES OF FOREIGN GOVERNMENTS 13 (Comm. Print 1962)).

33. See *id.*

34. See *Keene*, 619 F. Supp. at 1115.

35. See OFFICE OF THE INSPECTOR GEN., *supra* note 31, at 2.

36. See U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL § 2062, <https://www.justice.gov/archives/usam/criminal-resource-manual-2062-foreign-agents-registration-act-enforcement> (last updated Dec. 7, 2018).

37. See CYNTHIA BROWN, CONG. RESEARCH SERV., R45037, THE FOREIGN AGENTS REGISTRATION ACT (FARA): A LEGAL OVERVIEW (2017), <https://fas.org/sgp/crs/misc/R45037.pdf> (citing Lobbying Disclosure Act of 1995, Pub. L. No. 104-65, § 9, 109 Stat. 691, 699; Lobbying Disclosure Technical Amendments Act of 1997, Pub. L. No. 105-166, § 5, 112 Stat. 38, 39).

38. See H.R. REP. NO. 104-339, at 21 (1995); see also 22 U.S.C. § 613(h) (2012). FARA's registration requirements were limited in this way by requiring that the agent be involved in political activities "for or on behalf" of the foreign principal. See U.S. DEP'T OF JUSTICE, *supra* note 36.

39. 22 U.S.C. § 614(a).

40. See OFFICE OF THE INSPECTOR GEN., *supra* note 31, at 2-3.

R

R

R

The history of FARA criminal prosecutions and registrations reflects these shifting policy concerns. The first three prosecutions, which were brought in 1939 and 1940, involved the Soviet Union. From 1940 until the end of World War II, the government brought sixteen prosecutions, eleven involving Germany. Between the end of the war and 1963, DOJ reported twelve prosecutions, three of which involved the Soviet Union and five of which involved Cuba—again reflecting the propaganda threats to the U.S. at the time.⁴¹ Prosecutions then largely ceased, likely owing to the Act’s shifted focus onto lobbying, until FARA’s resurgence in 2017.⁴²

FARA registration numbers peaked in the 1980s, before the passage of the LDA, with a high of 916 active registrations in 1987. From the mid-1990s until about 2017, registration fell sharply, likely owing to the passage of the LDA and its FARA exception.⁴³ But in 2018, FARA saw a nearly twenty percent increase in registrations since 2017 and a forty-three percent increase since the end of 2014.⁴⁴ These recent numbers likely owe to the increased enforcement of FARA that will be detailed in the next Section.

While FARA enforcement has, as illustrated, changed considerably over the decades, it may need to return to some of its earlier roots if it is to be used as a tool against disinformation actors on social media. Today’s social media propogandists disseminate “political propaganda”—to use FARA’s earlier language⁴⁵—more than they disseminate legitimate “information materials,” as the Act is currently worded.⁴⁶ And while the LDA and other laws address foreign lobbying, FARA is currently the only law on the books capable of addressing foreign-based social media propagandists. FARA therefore may be uniquely suited to play a role in countering disinformation. The spread of disinformation, according to one scholar, is “the rare type of national security threat for which informing the public actually can diminish the threat: if Americans know what to look out for online and what not to accept at face value on social media, the power of dis-

41. See Attorney Gen. of U.S. v. Irish People, Inc., 684 F.2d 928, 945 (D.C. Cir. 1982) (citing *Activities of Nondiplomatic Representatives of Foreign Principals in the United States: Hearings Before the S. Comm. on Foreign Relations*, 88th Cong. 70–73 (1963)).

42. See Laufman, *supra* note 4.

43. See OFFICE OF THE INSPECTOR GEN., *supra* note 31, at 2.

44. See Laufman, *supra* note 4.

45. See *supra* note 27 for the definition of “political propaganda.”

46. See text accompanying *infra* note 182 for the current definition of “informational materials.”

R
R
R
R
R

information deliberately spread by hostile actors is reduced.”⁴⁷ As this Article will explore, FARA may be a useful tool in combatting disinformation—but to do so, it may be necessary to reconsider the ways in which DOJ enforces FARA registration.

Using FARA in this context, however, is admittedly not an easy fit. While FARA focuses on the fact that a certain political influence is foreign in nature, social media companies have different points of concern: Facebook is concerned chiefly with whether the origin of its content, wherever it is from, is transparent to users, and Twitter is focused less on the location of an account than on behavioral patterns that suggest accounts are gaming the system.⁴⁸ The reason for these differences includes the fact that it is often difficult to identify with a high degree of certainty where a social media account originates.⁴⁹ This Article will explore these tensions, and what they might mean for FARA’s applicability to social media actors, in more depth below.

B. FARA’s Recent Resurgence

FARA has recently appeared in the public consciousness on a number of occasions, even before the special counsel indicted a number of Russian disinformation actors under its provisions in 2018. In September 2017, DOJ asked T&R Productions LLC, the company that supplies broadcasting services to the U.S. affiliate of the state-owned Russian news outlet RT, formerly known as Russia Today, to register under FARA as a foreign agent.⁵⁰ DOJ officials argued that RT’s contracts made it clear that the network’s U.S. affiliates were under the control of TV Novosti, a Russian-government backed broadcaster.⁵¹ In a letter that DOJ sent to the network, officials claimed that financial information showed that in 2015, 99.7% of the funds expended by RT

47. See Joshua Geltzer, *The Most Extraordinary Lesson of Two New Reports on Russian Disinformation: What They Reveal About White House Paralysis*, JUST SECURITY (Dec. 17, 2018), <https://www.justsecurity.org/61908/extraordinary-lesson-reports-russian-disinformation-reveal-white-house-paralysis/>.

48. See Evelyn Douek, *Senate Hearing on Social Media and Foreign Influence Operations: Progress, but There’s a Long Way to Go*, LAWFARE (Sept. 6, 2018, 2:38 PM), <https://www.lawfareblog.com/senate-hearing-social-media-and-foreign-influence-operations-progress-theres-long-way-go>.

49. *Id.*

50. *US DOJ Uses WWII-Era Legislation to Demand That RT Supplier Register as a ‘Foreign Agent,’* RT, <https://www.rt.com/usa/402923-rt-foreign-agent-doj/> (last updated Sept. 12, 2017, 7:38 AM).

51. See Josh Gerstein, *DOJ Told RT to Register a Foreign Agent Partly Because of Alleged 2016 Election Interference*, POLITICO (Dec. 21, 2017, 10:42 AM), <https://www.politico.com/story/2017/12/21/russia-today-justice-department-foreign-agent-election-interference-312211>.

came from the Russian government.⁵² Russian President Vladimir Putin has explicitly said that “[RT] is funded by the [Russian] government, so it cannot help but reflect the Russian Government’s official position on the events in our country and in the rest of the world.”⁵³ In November 2017, DOJ announced RT’s registration, stating in a press release that “Americans have a right to know who is acting in the United States to influence the U.S. government or public on behalf of foreign principals.”⁵⁴

A Washington, D.C., radio station named Reston Translator, which broadcasts Russian state-funded news outlet Sputnik, registered with DOJ as a foreign agent in November 2017 as well.⁵⁵ These were not the first FARA registrations for Russian news outlets, though they are some of the most recent. The New York bureau of the Soviet news agency TASS, for example, was registered as a foreign agent from the 1940s onward, as were a number of other Soviet media outlets.⁵⁶ Russia has not been the only country whose media has been targeted for FARA registration. In September 2018, China’s Xinhua News Agency and China Global Television Network were also ordered to register under the law.⁵⁷

52. Letter from Heather H. Hunt, Chief, FARA Registration Unit, to Brian E. Dickerson, Attorney, RTTV America, Inc. 2–3 (Aug. 17, 2017), <https://www.politico.com/f/?id=00000160-79a9-d762-a374-7dfbebe30001>.

53. *Id.* at 3.

54. Press Release, U.S. Dep’t of Justice, Production Company Registers Under the Foreign Agent Registration Act as Agent for the Russian Government Entity Responsible for Broadcasting RT (Nov. 13, 2017), <https://www.justice.gov/opa/pr/production-company-registers-under-foreign-agent-registration-act-agent-russian-government>.

55. See Megan R. Wilson, *Russian News Outlet Sputnik Registers with DOJ as Foreign Agent*, HILL (Nov. 17, 2017, 1:15 PM), <http://thehill.com/business-a-lobbying/business-a-lobbying/360912-russian-news-outlet-sputnik-registers-with-doj-as>; Nathan Layne, *U.S.-Based Russian News Outlet Registers as Foreign Agent*, REUTERS (Feb. 17, 2018, 10:07 PM), <https://www.reuters.com/article/us-usa-trump-russia-propaganda/u-s-based-russian-news-outlet-registers-as-foreign-agent-idUSKCN1G201H>.

56. James Kirchick, *RT Wants to Spread Moscow’s Propaganda Here. Let’s Treat It that Way.*, WASH. POST (Sept. 20, 2017), https://www.washingtonpost.com/news/posteverything/wp/2017/09/20/rt-wants-to-spread-moscows-propaganda-here-lets-treat-it-that-way/?tid=A_inl&utm_term=.d6d318827e53.

57. Cristina Maza, *Why These Chinese Media Companies Have to Register as Foreign Agents*, NEWSWEEK (Sept. 19, 2018, 11:00 AM), <https://www.newsweek.com/why-these-chinese-media-companies-have-register-foreign-agents-1128649>. Note that units belonging to broadcasters and publications from Korea, Japan, and Canada have also registered under FARA at various times. See Mike Eckel, *U.S. Justice Department Says Intelligence Report Spurred FARA Requirement for RT*, RADIO FREE EUR./RADIO LIBERTY (Dec. 21, 2017, 4:02 PM), <https://www.rferl.org/a/russia-rt-fara-intelligence-report-us-justice-department/28931638.html>.

The recent uptick in FARA registrations and prosecutions has not been limited to foreign media outlets. Among other prominent cases, the special counsel repeatedly used FARA in his indictments of some of President Donald Trump's associates. In November 2017, the special counsel brought indictments against former Trump campaign chairman Paul Manafort and his deputy Richard Gates, charging them with FARA violations among other counts.⁵⁸ They were both accused of acting as agents of the Ukrainian government under Viktor Yanukovich, the pro-Russian former president, sending shockwaves through the lobbying world in what many have called the most significant FARA prosecution ever.⁵⁹ Additionally, Michael Flynn, President Trump's former National Security Advisor, filed paperwork under FARA in March 2017 as a foreign agent who was paid to do work for the Turkish government.⁶⁰ These cases have led to increased efforts by many foreign lobbyists to disclose their activities to avoid public scrutiny.⁶¹ All in all, the two-year period from 2017 to 2019 has seen nearly as many criminal prosecutions for FARA violations as during the forty-year period from 1966 to 2015.⁶²

The flurry of attention that FARA recently received led to the introduction of a series of reform bills in the Senate and the House. Among other bills, in March 2017, Senators Todd Young (R-IN) and Jeanne Shaheen (D-NH) introduced the Foreign Agents Registration Modernization and Enforcement Act, which would provide DOJ with the authority to investigate potential FARA violations and compel organizations to produce documentation to confirm funding sources and foreign connections.⁶³ In October 2017, Congressman Mike Johnson (R-LA) and Senator Chuck Grassley (R-IA) introduced the Disclosing Foreign Influence Act, which would reverse the 1995 decision to remove most private sector lobbying reporting from FARA to the

58. See Rosie Gray, *How the Manafort Indictment Gave Bite to a Toothless Law*, ATLANTIC (Oct. 30, 2017), <https://www.theatlantic.com/politics/archive/2017/10/how-the-manafort-indictment-gave-bite-to-a-toothless-law/544448/>.

59. *Id.*

60. Elliot Hannon, *Former National Security Adviser Flynn Registered as a Foreign Agent for Turkey Work During Trump Campaign*, SLATE (Mar. 8, 2017, 8:49 PM), http://www.slate.com/blogs/the_slatest/2017/03/08/flynn_registers_as_foreign_agent_with_justice_dept_for_turkey_work_during.html.

61. Masood Farivar, *Foreign Lobbyists Disclose Activities amid Increased Scrutiny*, VOA (Sept. 18, 2018, 10:25 PM), <https://www.voanews.com/a/foreign-lobbyists-disclose-activities-amid-increased-scrutiny-/4577744.html>.

62. See Laufman, *supra* note 4.

63. S. 625, 115th Cong. § 2 (2017); Press Release, Sen. Todd Young, Americans Deserve Media Transparency Not Propaganda (Mar. 15, 2017), <https://www.young.senate.gov/newsroom/press-releases/americans-deserve-media-transparency-not-propaganda>.

LDA.⁶⁴ At the time of this Article's publication, both of these bills have been referred to the Committee on Foreign Relations but have not yet been voted on.⁶⁵

More importantly, this burst of legislative activity aims to strengthen FARA's effectiveness with regard to lobbyists and non-anonymous sources of political influence. But these bills do not attempt to apply FARA to the types of social media actors that Special Counsel Mueller identified in his February 2018 indictment and October 2018 complaint. This Article therefore seeks to fill the void in both the scholarship and these legislative proposals by studying how FARA might apply to disinformation actors on social media. To contextualize the amendments to FARA that this Article will consider, it is necessary to first discuss the kinds of social media disinformation activity about which this Article is concerned. The next Section will briefly outline the nature of disinformation campaigns on social media, focusing primarily on the public evidence available regarding disinformation efforts during and after the 2016 presidential election.

II.

FOREIGN ORGANIZED DISINFORMATION CAMPAIGNS DURING AND AFTER 2016

Planting false news—or disinformation—in the press is not a new phenomenon. Indeed, such practices have existed since at least the eighteenth century. Benjamin Franklin, for instance, intentionally published untrue stories alleging that the British paid Native Americans to scalp men, women, and children in the rebellious colonies.⁶⁶ In 1835, a penny press paper, the *New York Sun*, ran a series of articles claiming that an astronomer, using a new high-powered telescope, discovered life on the moon. Owing to this hoax, the *Sun* became the most widely read newspaper in the world.⁶⁷ More recently, in the run-

64. S. 2039, 115th Cong. § 2 (2017); see Press Release, Rep. Mike Johnson, Rep. Johnson, Sen. Grassley Introduce Bill to Shine Light on Foreign Influences (Oct. 31, 2017), <https://mikejohnson.house.gov/media/press-releases/rep-johnson-sen-grassley-introduce-bill-shine-light-foreign-influences>.

65. S.625—*Foreign Agents Registration Modernization and Enforcement Act*, CONGRESS.GOV, <https://www.congress.gov/bill/115th-congress/senate-bill/625> (last visited Apr. 10, 2019) (showing “[l]atest [a]ction” taken on bill referral to the Committee on Foreign Relations); S.2039—*Disclosing Foreign Influence Act*, CONGRESS.GOV, <https://www.congress.gov/bill/115th-congress/senate-bill/2039> (last visited Apr. 10, 2019) (same).

66. Steven Seidenberg, *Fake News Has Long Held a Role in American History*, ABA JOURNAL (July 2017), http://www.abajournal.com/magazine/article/history_fake_news.

67. *Id.*

up to the Spanish-American War, William Randolph Hearst fabricated news stories to coax Americans into war.⁶⁸

During the Cold War, the United States and the Soviet Union engaged in an all-out ideological information war, but this information war seemed to end after the Soviet Union's collapse.⁶⁹ Congress and President Bill Clinton closed the United States' preeminent global information agency responsible for countering the propaganda threat, the United States Information Agency ("USIA"), in 1999.⁷⁰ Since Vladimir Putin's rise to power, reports suggest that Russia has been searching for new ways to make up for its diminished military, and officials have seized on influence campaigns and cyberwarfare as a cheap, easy-to-deploy means of re-achieving parity with the United States.⁷¹ Though Russia has been publicly identified as the most likely culprit behind the disinformation campaign in and around 2016, other countries, such as Iran, have been cited for using foreign propaganda as well.⁷² The tools that Russia allegedly used require few barriers to entry, making it likely that other countries or groups will follow suit.⁷³

Russian "active measures" on Facebook and other social media began long before the 2016 primary season⁷⁴ and in many cases have lasted long after the November 8, 2016, election.⁷⁵ The Russian opera-

68. *Id.*

69. 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.

70. See Mark Dillen, *The Decline and Fall of USIA Cover*, AM. DIPL. (Feb. 2013) (book review), <http://americandiplomacy.web.unc.edu/2013/02/the-decline-and-fall-of-usia-cover/>.

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

72. Craig Timberg et al., *Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation*, WASH. POST (Aug. 21, 2018), <https://www.washingtonpost.com/technology/2018/08/21/russian-iran-created-facebook-pages-groups-accounts-mislead-users-around-world-company-says/>.

73. Anne Applebaum, *If Russia Can Create Fake 'Black Lives Matter' Accounts, Who Will Next?*, WASH. POST (Oct. 15, 2017), https://www.washingtonpost.com/opinions/global-opinions/if-russia-can-create-fake-black-lives-matter-accounts-who-will-next/2017/10/15/ffb2e01e-af79-11e7-be94-fabb0f1e9ffb_story.html.

74. "Active measures" was the name originally given to KGB-run information and psychological warfare designed to win the battle for people's minds. See PETER POMERANTSEV & MICHAEL WEISS, INST. OF MODERN RUSS., *THE MENACE OF UNREALITY: HOW THE KREMLIN WEAPONIZES INFORMATION, CULTURE AND MONEY* 8 (2014), <http://www.interpretermag.com/wp-content/uploads/2015/07/PW-31.pdf>.

75. Ryan Goodman & Justin Hendrix, *Facebook Users Have the Right to Know How They Were Exposed to Russian Propaganda*, JUST SECURITY (Oct. 23, 2017), <https://www.justsecurity.org/46171/facebook-users-right-to-know-exposed-russian->

tion that began in 2016 went beyond just spreading false news and spamming;⁷⁶ the interference campaign also created and controlled real-world events.⁷⁷ The continuing interference's overarching goal appears to be to destabilize the United States by focusing on and amplifying existing tensions, rather than supporting any one political party.⁷⁸ Disinformation campaigns are an active measure tool which Russian intelligence has reportedly used since the Cold War to sow discord among and within countries Russia perceives as hostile to its interests.⁷⁹ Now that Facebook and Twitter have become dominant media platforms,⁸⁰ social media has become the new battleground on which these disinformation campaigns occur.

The Russian active measures used to spread disinformation operate both overtly and covertly.⁸¹ News channels like RT and Sputnik are two primary examples of overt means. While RT is primarily a news organization, it has benefitted considerably from social media's amplification of its articles. Consider RT's prominent presence on YouTube's search results, which has led it to attract 2.2 million subscribers.⁸² YouTube helped RT achieve such prominence by providing it with perks, like a "check mark" that designated RT as a verified

propaganda/. For one more recent example of Russia's continued use of these tools, see Sheera Frenkel & Daisuke Wakabayashi, *After Florida School Shooting, Russian 'Bot' Army Pounced*, N.Y. TIMES (Feb. 19, 2018), <https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html>.

76. *Spamming*, TECHOPEDIA, <https://www.techopedia.com/definition/23763/spamming> (last visited Mar. 10, 2019) (defined as sending unwanted bulk messages indiscriminately to online content sections on social media).

77. See, e.g., Sam Levin & Olivia Solon, *'Our Pain for Their Gain': The American Activists Manipulated by Russian Trolls*, GUARDIAN (Oct. 21, 2017, 7:00 AM), <https://www.theguardian.com/world/2017/oct/21/russia-social-media-activism-blacktivist>.

78. See Tom McCarthy, *How Russia Used Social Media to Divide Americans*, GUARDIAN (Oct. 14, 2017, 9:47 AM), <https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook> (quoting Jonathan Morgan, a former State Department advisor on digital responses to terrorism).

79. See Natasha Bertrand, *It Looks Like Russia Hired Internet Trolls to Pose as Pro-Trump Americans*, BUS. INSIDER (July 27, 2016, 8:23 AM), <http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7>.

80. See Alexis C. Madrigal, *What Facebook Did to American Democracy*, ATLANTIC (Oct. 12, 2017), <https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/>.

81. Some measures, such as a series of recently taken down online video channels that are backed by RT but do not disclose that they are funded by the Russian government, blur the line between overt and covert propaganda. See Donie O'Sullivan et. al., *Russia Is Backing a Viral Video Company Aimed at American Millennials*, CNN <https://www.cnn.com/2019/02/15/tech/russia-facebook-viral-videos/index.html> (last updated Feb. 18, 2019, 12:02 PM).

82. See Daisuke Wakabayashi & Nicholas Confessore, *Russia's Favored Outlet Is an Online News Giant. YouTube Helped.*, N.Y. TIMES (Oct. 23, 2017), https://www.nytimes.com/2017/10/23/technology/youtube-russia-rt.html?_r=1.

news source, and including RT among a select group of news organizations in Google's "preferred" news lineup.⁸³ This granted RT access to guaranteed revenue from premium advertisers, in effect subsidizing this international propaganda arm.⁸⁴ To date, there have been over five billion views of RT's online videos.⁸⁵

While YouTube may be facilitating foreign media entities like RT, other social media companies, like Twitter, have been exploited by covert means of influence. One such covert means is the use of "bots," software applications that perform automated tasks on the Internet.⁸⁶ Some researchers estimate that up to twenty-three percent of Twitter accounts are bots.⁸⁷ At one point in summer 2016, 17,000 bot accounts amplified Russia's disinformation efforts, and in August 2017, more than 75,000 bots responded to a researcher's post seeking to trigger such a response.⁸⁸ These bots are able to amplify messages to a degree not possible for human beings, averaging more than 1,500 tweets per day.⁸⁹ Given the ease of automated abuse on its platform, even Twitter probably does not know the extent to which foreign entities have been using bots on the site.⁹⁰ Twitter CEO Jack Dorsey has himself retweeted an account that was identified as Kremlin-created by an independent Russian news agency.⁹¹

Russian-based entities have also engaged in the covert active measure of "trolling," deliberately using online fora for provocations designed to cause quarreling and discord.⁹² Members of the St. Petersburg-based privately-owned Internet Research Agency ("IRA") posed as U.S. persons and created false U.S. personas online, operating so-

83. *Id.*

84. *See id.*

85. *See* Evelyn Douek, Summary of Congressional Tech Hearings 27 (Jan. 11, 2018) (unpublished notes), <https://www.lawfareblog.com/congress-grilling-tech-companies-2017-foreshadows-debates-2018> (follow "my longer account" hyperlink).

86. Sarah Mitroff, *What Is a Bot? Here's Everything You Need to Know*, CNET (May 5, 2016, 3:23 PM), <https://www.cnet.com/how-to/what-is-a-bot/>.

87. *See* Zhouhan Chen et. al., *Hunting Malicious Bots on Twitter: An Unsupervised Approach* (Sept. 2, 2017) (unpublished conference paper) (on file with author).

88. *See* Thomas Rid, *Why Twitter Is the Best Social Media Platform for Disinformation*, MOTHERBOARD (Nov. 1, 2017, 8:00 AM), https://motherboard.vice.com/en_us/article/bj7vam/why-twitter-is-the-best-social-media-platform-for-disinformation.

89. *Id.*

90. *See id.*

91. Ben Collins, *Twitter CEO Jack Dorsey Retweeted Alleged Russian Trolls*, DAILY BEAST (Oct. 20, 2017, 6:08 PM), <https://www.thedailybeast.com/twitter-ceo-retweeted-alleged-russian-trolls>.

92. *Troll*, TECHOPEDIA, <https://www.techopedia.com/definition/429/troll> (last visited Mar. 10, 2019).

cial media pages and groups designed to attract U.S. audiences.⁹³ The “specialists” employed by the IRA, who created these social media accounts, were divided into day and night shifts to post within the appropriate U.S. time zone, and were circulated a list of U.S. holidays so that they could post appropriate corresponding activity.⁹⁴ The organization also purchased advertisements on social media sites to promote its pages and groups.⁹⁵

The trolling extended beyond Internet activity to real-life action, including the co-opting of unknowing Americans to serve as the IRA’s agents from abroad. Reportedly, Russian operatives even paid American activists in the planning of events.⁹⁶ For example, in both 2016 and 2017, the “American Department,” or “translator project,” of the IRA allegedly recruited U.S. activists to help stage protests and organize self-defense classes in black communities to sow division among Americans.⁹⁷ In one instance, operators spoke by telephone with a real U.S. person affiliated with a grassroots group in Florida.⁹⁸ The IRA also allegedly operated Facebook pages, such as the Heart of Texas, which called for Texas’s secession from the United States and promoted anti-Muslim rallies.⁹⁹ Russian-operated sites, such as Blacktivist, were reported to have taken proactive roles in communicating with activists, confusing even bona fide activists about their actual origins.¹⁰⁰ On some occasions, the foreign account operators used real people, impersonating certain Americans as avatars to deliver their

93. See Indictment ¶ 10.

94. See *id.* ¶ 33.

95. See *id.* ¶ 35.

96. See Rosalind Adams & Hayes Brown, *These Americans Were Tricked into Working for Russia. They Say They Had No Idea.*, BUZZFEED NEWS (Oct. 17, 2017, 10:34 PM), <https://www.buzzfeed.com/rosalindadams/these-americans-were-tricked-into-working-for-russia-they>; see also Indictment ¶ 54 (charging that the Internet Research Agency “offered money to certain U.S. persons to cover rally expenses.”).

97. Indictment ¶ 10; Donie O’Sullivan, Drew Griffin & Curt Devine, *In Attempt to Sow Fear, Russian Trolls Paid for Self-Defense Classes for African Americans*, CNN (Oct. 18, 2017, 9:30 PM), <https://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html>.

98. See Indictment ¶ 82.

99. Secession was also a popular subject for RT America, which featured a six-minute story on the subject in June 2016 that received 250,000 views on YouTube. See Tim Lister & Clare Sebastian, *Stoking Islamophobia and Secession in Texas—from an Office in Russia*, CNN, <http://www.cnn.com/2017/10/05/politics/heart-of-texas-russia-event/index.html> (last updated Oct. 6, 2017, 5:00 PM).

100. See Sam Levin, *Did Russia Fake Black Activism on Facebook to Sow Division in the US?*, GUARDIAN (Sept. 30, 2017, 6:00 AM), <https://www.theguardian.com/technology/2017/sep/30/blacktivist-facebook-account-russia-us-election>.

talking points,¹⁰¹ as well as creating accounts such as “the United Muslims of America” on Facebook to impersonate an actual but currently non-functional organization.¹⁰² The content from these and other allegedly Russian-operated sites was reportedly shared 340 million times,¹⁰³ with the IRA allegedly publishing as many as 50 million posts a month in 2016.¹⁰⁴ While the IRA is the best-known and to this day the only indicted Russian “troll farm,” independent journalists in Russia estimate that there are hundreds of others,¹⁰⁵ and some reports suggest that other accounts were “likely more important in spreading fake news.”¹⁰⁶ Facebook estimates that the activities of these entities reached nearly 150 million users.¹⁰⁷ Twitter notified 677,775 people in the United States who either followed, retweeted, or liked a tweet from troll IRA accounts.¹⁰⁸

While most of this allegedly Russian activity was coordinated from abroad, some was conducted within the United States. IRA affiliates traveled to the United States under false pretenses to collect intelligence to inform its operations.¹⁰⁹ The IRA also used computer

101. See, e.g., Spencer Ackerman et al., *Russia Recruited YouTubers to Bash ‘Racist B*tch’ Hillary Clinton over Rap Beats*, DAILY BEAST (Oct. 8, 2017, 9:00 PM), <https://www.thedailybeast.com/russia-recruited-youtubers-to-bash-racist-btch-hillary-clinton-over-rap-beats>.

102. See Kevin Poulsen et al., *Exclusive: Russians Impersonated Real American Muslims to Stir Chaos on Facebook and Instagram*, DAILY BEAST (Sept. 27, 2017, 4:29 PM), <https://www.thedailybeast.com/exclusive-russians-impersonated-real-american-muslims-to-stir-chaos-on-facebook-and-instagram>; see also Indictment ¶ 34.

103. Goodman & Hendrix, *supra* note 75.

104. See Alexey Kovalev, *Russia’s Infamous ‘Troll Factory’ Is Now Posing as a Media Empire*, MOSCOW TIMES (Mar. 24, 2017), <https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534> (reporting secondhand that the Federal News Agency (“FAN”), a moniker interchangeable with the IRA, wrote as many as 50 million posts a month).

105. See Goodman & Hendrix, *supra* note 75.

106. Knight Found., *Seven Ways Misinformation Spread During the 2016 Election*, MEDIUM (Oct. 4, 2018), <https://medium.com/trust-media-and-democracy/seven-ways-misinformation-spread-during-the-2016-election-a45e8c393e14> (reporting that several other Twitter accounts were posting content similar to the IRA but had many more followers than the top IRA trolls).

107. See Spencer Ackerman, *Facebook Now Says Russian Disinfo Reached 150 Million Americans*, DAILY BEAST (Nov. 1, 2017, 12:38 PM), <https://www.thedailybeast.com/facebook-now-says-russian-disinfo-reached-150-million-americans>. The 150 million user estimate accounts for users of both Facebook and Instagram, which Facebook owns. *Id.*

108. Ashley Gold, *Twitter: More than 677,000 U.S. Users Engaged with Russian Troll Accounts*, POLITICO (Jan. 19, 2018, 6:16 PM), <https://www.politico.com/story/2018/01/19/twitter-users-russian-trolls-437247>.

109. See Indictment ¶ 5. Note that Congress has introduced legislation that would seek to block such foreigners from entering the United States. See SECURE Our Democracy Act, H.R. 6494, 115th Cong. (2018).

R

R

infrastructure inside the United States.¹¹⁰ For example, a company owned by a man in Staten Island, New York, provided internet infrastructure services to a Russian propaganda site pretending to be a voice for victims of police shootings.¹¹¹ A former FBI agent who is an expert on Russian disinformation campaigns suggests that the use of Russian communities within the United States as website hosts is typical behavior, designed to create anonymity and make the source look authentic.¹¹²

The IRA also purchased space on computer servers located in the United States to set up virtual private networks (“VPNs”) through which operators in Russia could connect to the U.S.-based infrastructure and conduct their activity inside the United States.¹¹³ Other kinds of American involvement straddle a blurrier line between foreign influence and domestic First Amendment protected political opinion, such as the former *Breitbart* reporter Lee Stranahan whom Sputnik hired to start a radio show in Washington, D.C.¹¹⁴ In response to accusations, Stranahan said that although his paycheck comes from the Russians, “nothing about it really affects my position on stuff that I’ve had for years now.”¹¹⁵

This disinformation campaign continued past the 2016 election cycle. Six hundred Twitter accounts reportedly linked to Russian influence operations were found promoting extremism around the time of the Charlottesville protest in the summer of 2017.¹¹⁶ In the fall of 2018, bot and troll activity increased in response to the confirmation

110. See Katie Zavadski et al., *Exclusive: Russian Propaganda Traced Back to Staten Island, New York*, DAILY BEAST (Oct. 23, 2017, 9:57 PM), <https://www.thedailybeast.com/russian-propaganda-hosted-by-man-on-staten-island-new-york>.

111. *Id.* In addition, a California man was sentenced to six months in prison for selling bank account information that Russia used in its disinformation campaign. See Sharon LaFraniere, *Californian Who Unwittingly Aided Russian Election Interference Gets 6 Months in Prison*, N.Y. TIMES (Oct. 10, 2018), <https://www.nytimes.com/2018/10/10/us/politics/richard-pinedo-sentencing-mueller.html>.

112. Zavadski et al., *supra* note 110 (“You don’t want these to trace back to Russia, so you pick a believable community closest to your target. It’s not necessarily that they’re directed Russian agents, but they can go through Russian communities—witting or unwitting—outside of Russia.”).

113. See Indictment ¶ 39.

114. See Rosie Gray, *From Breitbart to Sputnik*, ATLANTIC (Apr. 5, 2017), <https://www.theatlantic.com/politics/archive/2017/04/from-breitbart-to-sputnik/522051/>.

115. *Id.*

116. See Isaac Arnsdorf, *Pro-Russian Bots Take up the Right-Wing Cause After Charlottesville*, PROPUBLICA (Aug. 23, 2017, 8:00 AM), <https://www.propublica.org/article/pro-russian-bots-take-up-the-right-wing-cause-after-charlottesville> (“A sample of 600 Twitter accounts linked to Russian influence operations have been promoting hashtags for Charlottesville . . .”).

battle concerning Justice Kavanaugh's nomination to the Supreme Court.¹¹⁷ The highest peak of IRA ad volume on Facebook was actually April 2017,¹¹⁸ and according to experts, bot activity on Twitter has increased since the 2016 election.¹¹⁹ One cybersecurity company detected more overall activity from Russian online influence operations targeting the 2018 midterm elections than was detected by researchers during the same period before the 2016 election.¹²⁰

Disinformation has also become harder to find as tactics change. The focus has shifted from propagating fake news stories to, in the words of a cybersecurity firm executive, "augmenting stories already out there which speak to hyperpartisan audiences."¹²¹ As Facebook stated in a summer 2018 press release, "[S]ecurity is not something that's ever done. . . . It's an arms race and we need to constantly improve too."¹²²

III.

MODERNIZING THE FOREIGN AGENTS REGISTRATION ACT

The social media disinformation campaign described in the previous Part represents a type of propaganda threat that in many ways is more like the old-fashioned phenomenon of subversive sign-holding propagandists that existed when FARA was adopted than the more recent phenomenon of foreign lobbyists. While today's disinformation actors behave in many ways like traditional propagandists, the tools

117. See Max de Haldevang, *Russian Trolls and Bots Are Flooding Twitter with Ford-Kavanaugh Disinformation*, QUARTZ (Oct. 2, 2018), <https://qz.com/1409102/russian-trolls-and-bots-are-flooding-twitter-with-ford-kavanaugh-disinformation/> (reporting that the CEO of information integrity firm New Knowledge believed that the Kavanaugh confirmation resulted in more U.S. propaganda from foreign sources than the firm had seen in months).

118. Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018*, at 3 (2018) (Univ. of Oxford Computational Propaganda Research Project, Working Paper No. 2018.2, 2018), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>.

119. See Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html> (quoting former FBI agent's observation that Facebook had begun to address their bot problem while Twitter had not).

120. Jonathon Morgan & Ryan Fox, Opinion, *Russians Meddling in the Midterms? Here's the Data*, N.Y. TIMES (Nov. 6, 2018), <https://www.nytimes.com/2018/11/06/opinion/midterm-elections-russia.html>.

121. Sheera Frenkel & Mike Isaac, *Inside Facebook's Election 'War Room,'* N.Y. TIMES (Sept. 19, 2018), <https://www.nytimes.com/2018/09/19/technology/facebook-election-war-room.html>.

122. *Removing Bad Actors on Facebook*, FACEBOOK NEWSROOM (July 31, 2018), <https://newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/>.

they use and the platforms on which they operate are vastly different. To address this new category of actors, FARA would have to be enforced in ways it has never been before. This Part will explore the ways in which FARA could be used and adapted to address social media disinformation actors operating from abroad.

A. *The Agent and Foreign Principal Relationship in the Social Media Context*

Applying FARA to foreign-based social media disinformation campaigns poses a number of statutory challenges. First, FARA applies to an agent who “engages . . . *within* the United States in political activities for or in the interests of [a] foreign principal” (emphasis added),¹²³ but foreign social media propaganda agents are operating from abroad, not from “within” the United States. Second, FARA defines a foreign principal as any “person outside of the United States,”¹²⁴ referring to the traditional paradigm where a foreign country sends an agent inside the United States to influence its political process. This paradigm gives no guidance, however, as to how to distinguish social media agents operating from abroad from their foreign principals, who also operate from abroad. Third, the relationship between those operating behind the computer screen and the entities from which they may be taking direction is often more complicated and attenuated than the simple principal-agent relationship that FARA envisioned, requiring an analysis of the law of agency in the context of these social media actors. This Section will address each of these issues in turn.

The first issue, concerning the situs of the agent, is not unique to FARA. In a similar vein, determining the venue for network crimes has confounded federal courts because “in today’s wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused’s actual presence.”¹²⁵ In some of these cases, courts have found that venue may lie “where the effects of the defendant’s conduct are felt, but only when Congress has defined the essential conduct elements in terms of those effects.”¹²⁶ Applying this reasoning, it may be sufficient to say that a foreign-based social media operator is acting “within the United States,” as the Act requires, when

123. 22 U.S.C. § 611(c)(1)(i) (2012).

124. *Id.* § 611(b)(2).

125. *United States v. Saavedra*, 223 F.3d 85, 86 (2d Cir. 2000).

126. *United States v. Bowens*, 224 F.3d 302, 314 (4th Cir. 2000).

the effects of the operator's actions are felt within the United States. Moreover, Congress has seemingly defined the essential conduct elements in terms of those effects. The statutory language of acting "within" the United States first and foremost serves to narrow FARA to apply to foreign propaganda affecting *American* political opinion, as opposed to *foreign* political opinion; the statute does not indicate that the language was intended to establish the importance of the propagandist's physical location. Alternatively, the statutory language could be amended to "engages in political activities *aimed at* the United States" to more explicitly define the statutory conduct elements in these terms.¹²⁷

The second issue raised above, differentiating between the agent and principal when both actors are likely located abroad, makes the statute an uneasy fit for the kind of propagandists concerned here but does not pose an insurmountable obstacle. Given the opaque and non-linear structure behind foreign disinformation campaigns, it would be challenging to tie these statutory definitions to a particular, predetermined principal-agent relationship. But if both the agent and the principal are foreign-based, there is no meaningful significance in distinguishing the two. Any Russian "agent" operating on foreign soil is also, technically, a Russian "foreign principal." Whether defined as an "agent" or as a "principal," that actor would likely be subject to FARA registration either way.¹²⁸ FARA only expressly contemplates the registration of agents because at the time of its enactment, the agents were the front-line propagandists seeking to influence U.S. politics. Today, if agents have become interchangeable with their foreign principals because they are both located abroad, this distinction no longer matters.¹²⁹

127. Note that the definition of "political activities" in 22 U.S.C. § 611(o) remains important. It is limited to those activities that "the person engaging in believes will, or that the person intends to, in any way influence" the U.S. government or any section of the public to change U.S. domestic or foreign policy, ensuring that not every foreign commentator on U.S. politics is required to register under FARA. Only those foreign actors on social media that aim to influence U.S. policy, in the traditional political propaganda sense, would be required to register if FARA were to apply to these actors.

128. At times, there can be multiple foreign principals involved. For example, the IRA is allegedly funded by Concord Management and Concord Catering, which are allegedly controlled by Russian oligarch Yevgeny Prigozhin. While the hierarchy is complex, both Concord entities and the IRA would fall under FARA. *See generally* Clark et al., *supra* note 1.

129. In fact, recent media reports suggest that the principal-agent distinction has started to matter less in the lobbying context as well. *See* Natasha Bertrand, *A Surge in Foreign-Influence Prosecutions*, ATLANTIC (Dec. 18, 2018), <https://www.theatlantic.com/politics/archive/2018/12/michael-flynn-ex-associates-charged-turkey-lobby->

Still, where the U.S. government was attempting to make a case that a specific entity on social media was acting on behalf of a specific foreign principal, the question of agency remains an important one. Is the relationship between the coordinators and the operators of social media disinformation campaigns too nebulous to even qualify as legal agency? Under the Act's current language, FARA covers a broad range of possible agency relationships. FARA's disclosure and record-keeping requirements are imposed on "persons" who act as "agents of a foreign principal."¹³⁰ A "person" is defined as "an individual, partnership, association, corporation, organization, or any other combinations of individuals."¹³¹ Such a "person" is an "agent of a foreign principal" when the person "acts as an agent, representative, employee, or servant, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign principal."¹³² DOJ regulations have not further clarified the necessary elements of an agent's relationship with a foreign principal, but they have defined "control" to include "the possession or the exercise of power, directly or indirectly, to determine the policies or the activities of a person, whether through . . . contract, or otherwise."¹³³

The minimal case law that exists interpreting the Act suggests that this principal-agent relationship does not require that the parties expressly enter into a contract establishing the relationship.¹³⁴ While financial support from a foreign principal alone is insufficient to establish agency,¹³⁵ financial support is not required to establish agency.¹³⁶ The Act also does not include any threshold requirements for a certain degree of activity on the agent's part.

Beyond these general contours, the courts disagree on the standard by which a principal-agent relationship is established. The Third

case/578407/ (discussing how both the foreign principal who hired Michael Flynn's firm, Alptekin, and the alleged agents of the principal, Flynn and his U.S. business partner Kian, have been held accountable for allegedly lying about Flynn's government backers in an effort to falsify a FARA filing).

130. 22 U.S.C. § 612(a).

131. *Id.* § 611(a).

132. *Id.* § 611(c)(1).

133. 28 C.F.R. § 5.100(b) (2018).

134. *See* *United States v. German-American Vocational League, Inc.*, 153 F.2d 860, 863–64 (3d Cir. 1946) ("We find nothing in [the Act] . . . warranting the contention that it contemplated only agencies created by an express contract.").

135. *See* *Attorney Gen. of U.S. v. Irish People, Inc.*, 796 F.2d 520, 524 (D.C. Cir. 1986) (explaining that the Act was not intended to reach agents who are subsidized by foreign principals but do not act at the direction of foreign principals).

136. *See* *Attorney Gen. of U.S. v. Irish People, Inc.*, 595 F. Supp. 114, 118 (D.D.C. 1984), *aff'd in part, rev'd in part*, 796 F.2d 520 (D.C. Cir. 1986) (explaining that there "is no distinction made by FARA . . . between paid and unpaid agents").

Circuit Court of Appeals in 1945 applied the common law standard from the Restatement (First) of Agency, where agency is defined as “the relationship which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act.”¹³⁷ In 1981, the Second Circuit Court of Appeals, without citing the Third Circuit’s prior decision, favored a more FARA-specific definition concerned not with “whether the agent can impose liability upon his principal but whether the relationship warrants registration by the agent to carry out the informative purposes of the Act.”¹³⁸ The court cautioned that a broader reading, such as any person who acts at a foreign principal’s “request,” would “sweep within the statute’s scope many forms of conduct that Congress did not intend to regulate.”¹³⁹ In commenting on the proposed 1966 amendments, the House Report stated:

Under existing law it is possible because of the broad scope of the definitions contained in section 1(c) to find an agency relationship (and thus the possibility of registration) of persons who are not, in fact, agents of foreign principals but whose acts may incidentally be of benefit to foreign interests, even though such acts are part of the normal exercise of those persons’ own rights of free speech, petition, or assembly. This may have been desirable when the Foreign Agents Registration Act was amended in 1942, but does not appear warranted in present circumstances.¹⁴⁰

The court went on to state that the “surrounding circumstances” will usually provide sufficient indication as to whether a “request” by a foreign principal requires the recipient to register.¹⁴¹ The court provided two guidelines for what the “surrounding circumstances” might be. First, the court suggested that it is important to ascertain whether “those requested to act were identified with specificity by the principal;” specifically, whether “a particular individual, or a sufficiently limited group of identifiable individuals, is asked to act.”¹⁴² Second, the court suggested that the specificity of the action requested is relevant: “Once a foreign principal establishes a particular course of conduct to be followed, those who respond to its ‘request’ for complying action may properly be found to be agents under the Act.”¹⁴³

137. *German-American Vocational League, Inc.*, 153 F.2d at 869 n.9.

138. *Attorney Gen. of U.S. v. Irish N. Aid Comm.*, 668 F.2d 159, 161 (2d Cir. 1982).

139. *Id.*

140. *Id.* at 161 n.5 (citing H.R. REP. NO. 89-1470, at 6 (1966)).

141. *Id.* at 161.

142. *Id.*

143. *Id.* at 161–62.

Ultimately, determining whether agency exists for FARA registration purposes depends on the nature of the agent at issue. If the agent is a foreign national, then, as discussed above, he or she is technically both an “agent” and a “foreign principal” and would likely fall under FARA’s sweep either way. If the agent is an American citizen responding to a foreign national’s call to action, Congress’s concerns from 1966 come into play and DOJ would want to ensure that such an American citizen was acting specifically as an agent of a foreign principal under the Second or Third Circuit tests. Finally, if the concern is attributing a *specific* foreign agent to a *specific* foreign principal, a fact-specific investigation would be necessary to determine whether the relationship qualifies as agency under FARA.¹⁴⁴

For example, consider whether the IRA counts as an “agent” of a specific “foreign principal,” allegedly the Russian government. In a seminal paper that provides a useful model on the relationship between malicious online actors and nation-state sponsors, cybersecurity scholar Jason Healey describes a spectrum that measures the degree of state responsibility for cyber-attacks.¹⁴⁵ Alex Stamos, Facebook’s former chief security officer, concluded that the 2016 IRA activity is between “state-encouraged” and “state-ordered,” using Healey’s definitions.¹⁴⁶ Based on the Second Circuit test described above, either of these standards would be legally sufficient to determine that the IRA was an “agent” of the Russian state. But whether DOJ would choose to publicly disclose that an online campaign is attributable to a specific foreign principal would also depend in part on the most recent Department guidelines, which establish that “[f]oreign influence operations will be publicly identified as such only when the Department can attribute those activities to a foreign government with high confidence.”¹⁴⁷ Below, this Article will explore whether attributions with high confidence are possible in the social media context.

144. For example, the October 2018 criminal complaint alleges that Elena Alekseevna Khusyaynova was the chief accountant in the Russian operation to influence the 2016 and 2018 elections, suggesting that the IRA could be understood to be her “agent” to which she gave instructions for FARA purposes. *See generally* Clark et al., *supra* note 1.

145. JASON HEALEY, ATL. COUNCIL, BEYOND ATTRIBUTION: SEEKING NATIONAL RESPONSIBILITY FOR CYBER ATTACKS 2–4 (2012), https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

146. *Removing Bad Actors on Facebook*, *supra* note 122.

147. U.S. DEP’T OF JUSTICE, JUSTICE MANUAL, CRIMINAL RESOURCE MANUAL § 9-90.730, <https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730> (last visited Mar. 12, 2019).

R

R

B. Attribution in the Social Media Context

When it comes to adapting FARA to disinformation actors on social media, distinguishing who is the agent and who is the foreign principal is less challenging than resolving a more fundamental issue: is it even possible to identify, with any degree of certainty, who these social media operatives are? Can a Facebook page or Twitter account be attributed to a specific foreign actor with high confidence? Unlike public television station and social media channels like RT and Sputnik, bots and trolls on social media seek to hide their identity by design. The IRA, for example, registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names to mask the activity's Russian origin.¹⁴⁸ The Kremlin uses third-party contractors from both inside Russia and surrounding countries with cheap labor to “muddy the waters on attribution,” according to one former official.¹⁴⁹ This poses a difficulty when it comes to determining whether these operatives should be required to register under FARA.

Generally speaking, there are two possible kinds of attribution when it comes to actors on social media: direct attribution and indirect attribution. Direct attribution occurs when an entity can be identified by tracking its IP address, payments, or some other form of evidence that directly links the actor to the act.¹⁵⁰ Indirect attribution, carried out by research experts who do not have access to identifying information like IP addresses or payments, can be done by comparing social media identities across platforms and watching for common themes.¹⁵¹

The special counsel's 2018 indictment pointed to a number of the IRA's identifying features that represent the hallmarks of direct attribution. The indictment identified and named (1) Concord Management, a company that funded the organization's operations,¹⁵² (2) a number of Russian entities through which the IRA attempted to shield its identity,¹⁵³ and (3) a number of high-up individuals within the organization.¹⁵⁴ In one particularly revealing claim, the indictment cites

148. See Indictment ¶ 40.

149. See Ackerman et al., *supra* note 101.

150. See *generally* Indictment ¶¶ 10–24.

151. A prominent example of this kind of effort is Maltego, an interactive data mining tool that renders directed graphs for analysis of relationships between pieces of information from various online sources. See *Maltego CE*, PATERVA, <https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php> (last visited Mar. 12, 2019).

152. Indictment ¶ 3.

153. *Id.* ¶ 7.

154. *Id.* ¶¶ 10–24.

an email from a social media account operative to a family member saying, “we had a slight crisis here at work: the FBI busted our activity (not a joke).”¹⁵⁵

The government’s indictment further links these actors’ activities to the purchase of fake identification documents including drivers’ licenses,¹⁵⁶ and the use of the same fake personas that were deployed on social media to register for PayPal accounts. Some of the operatives purchased credit card and bank account numbers from online sellers using the stolen identities of real U.S. persons, which they then submitted to PayPal to evade its security measures.¹⁵⁷ The operatives would then use these accounts to purchase advertisements on Facebook to promote the IRA’s social media accounts.¹⁵⁸ The indictment also notes that many of these social media accounts were then deactivated,¹⁵⁹ further evidencing their involvement in the campaign.

Twitter has echoed some of the claims in the indictment by disclosing that it identifies Russian-linked accounts by looking at whether the account was created in Russia, “whether the user registered the account with a Russian phone carrier or a Russian email address, whether the user’s display name contains Cyrillic characters, . . . , and whether the user has logged in from any Russian IP address.”¹⁶⁰ Twitter’s acting general counsel, Sean Edgett, told Congress that because of “the information we have behind the scenes,” Twitter can directly connect collectives of autonomous accounts.¹⁶¹ Facebook’s former general counsel, Colin Stretch, similarly told members of Congress that “the technical signals [that we get from an account] can be used to help us identify inauthentic behavior.”¹⁶² But Facebook’s former chief security officer, Alex Stamos, cautions that using technical forensics does not always result in direct attribution with sufficiently high confidence.¹⁶³

Beyond these types of direct attribution, which reports suggest are typically available only to the government through intelligence

155. *Id.* ¶ 58.

156. *Id.* ¶ 41.

157. *Id.* ¶¶ 90–94.

158. *Id.* ¶ 94.

159. *Id.* ¶ 58.

160. See *Russia Investigative Task Force Open Hearing with Social Media Companies: Hearing Before the H. Permanent Select Comm. on Intelligence*, 115th Cong. 9 (2017) (testimony of Sean J. Edgett, Acting Gen. Counsel, Twitter, Inc.), <https://docs.house.gov/meetings/IG/IG00/20171101/106558/HHRG-115-IG00-Wstate-EdgettS-20171101.pdf>.

161. Douek, *supra* note 85, at 30.

162. *Id.* at 15.

163. See generally *Removing Bad Actors on Facebook*, *supra* note 146.

collection and to social media companies by way of their access to information about a user's account, indirect attribution is more difficult but also feasible. Researchers use Twitter's Search and Streaming API and Twitter Firehose to access and monitor trends on social media as they occur.¹⁶⁴ Other commonly used tactics involve geotagging,¹⁶⁵ analysis of language use,¹⁶⁶ and linkage of current accounts with prior accounts.¹⁶⁷ Cookies also serve as useful tools in tracking a user's actions across platforms online.¹⁶⁸ In identifying bots, certain data points, such as the number of times an account posts per day, the amount of personal details an account includes in its description, the number of times an account retweets other posts and the number of times it gets retweeted, and the nature of the Twitter handle, help separate human accounts from automatic ones.¹⁶⁹

Social media researchers generally suggest three As for spotting a fake account: "activity," "anonymity," and "amplification."¹⁷⁰ The "Botometer" monitors the activity of a Twitter account and gives it a score based on how likely it is to be a bot, using many of the factors listed above.¹⁷¹ An organization called Hamilton 68 tracked Russian influence operations on Twitter by watching 600 suspicious ac-

164. See Sarah Perez, *Twitter Launches Lower-Cost Subscription Access to Its Data Through New Premium APIs*, TECHCRUNCH (Nov. 14, 2017), <https://techcrunch.com/2017/11/14/twitter-launches-lower-cost-subscription-access-to-its-data-through-new-premium-apis/>.

165. See *Anatomy of a Russian Propaganda Troll: Geotagging Marks the Spot, Is It PROPAGANDA OR NOT?* (Mar. 24, 2017), <http://www.propornot.com/2017/03/anatomy-of-russian-propaganda-troll.html>.

166. See Kamil Baraniuk, *Corpus-Based Analysis as a Method to Identify Russian Trolling Activity*, 46 POLISH POL. SCI. Y.B. 239, 241 (2017), <http://www.marszalek.com.pl/yearbook/docs/46-1/ppsy2017115.pdf>.

167. See J.J. Patrick, *We Need to Talk About Identifying Trolls*, BYLINE (Nov. 13, 2017), <https://www.byline.com/column/67/article/1939>.

168. See Peter Eckersley, *How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them)*, ELECTRONIC FRONTIER FOUND. (Sept. 21, 2009), <https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks>.

169. See Ben Nimmo, *#BotSpot: Twelve Ways to Spot a Bot*, MEDIUM (Aug. 28, 2017), <https://medium.com/dfirlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c>. Accounts that post news headlines without providing links to the actual stories also usually suggest bot activity. See also James Devitt, *How to Detect Russian Bots on Twitter*, FUTURITY (Dec. 18, 2017), <http://www.futurity.org/russian-bots-twitter-1633842/>.

170. See Lauren C. Williams, *Where Are They Now? The Russian Bots That Disrupted the 2016 Election*, THINKPROGRESS (May 5, 2017, 1:53 PM), <https://thinkprogress.org/russian-bots-where-are-they-now-e2674c19017b/>.

171. See *FAQ*, BOTOMETER, <https://botometer.iuni.iu.edu/#!/faq> (last visited Mar. 12, 2019).

counts.¹⁷² Researchers using machine learning claim to be ninety-five percent accurate, with most of the errors being false negatives, i.e., troll accounts that were missed, rather than false positives, i.e., real accounts incorrectly classified as trolls.¹⁷³

While researchers have a number of tools at their disposal to make plausible inferences about an account's origin, and are working to improve their efforts, accurate identifications can be made with any degree of confidence only through direct attribution efforts like those evidenced by the U.S. government in its indictment and complaint, and through work done by the social media companies themselves. Nonetheless, it is hard to determine whether the kind of evidence that has been gathered against the IRA is available for any of the other organizations and groups that allegedly were involved in this Russian disinformation campaign or will be involved in others.¹⁷⁴

Moreover, actors caught in the 2016 campaign have likely already changed their tactics in preparation for their next influence campaigns.¹⁷⁵ For example, the IRA in 2016 made the "mistake" of buying some advertisements directly without use of a shell company;¹⁷⁶ now, it is more likely that entities will use shell companies to obscure their involvement. The upshot is that identification of the individuals behind the keyboard may always be impossible, and only the government and social media companies, who must work hard to keep up with the shifting disinformation tactics, have a real shot at attempting to attribute accounts to specific foreign entities with some degree of confidence.

172. See Laura Rosenberger & J.M. Berger, *Hamilton 68: A New Tool to Track Russian Disinformation on Twitter*, (Aug. 2, 2017), <https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/>.

173. See conspirator0, *Identifying Political Bot/Troll Social Media Activity Using Machine Learning*, MEDIUM (June 25, 2017), <https://medium.com/@conspirator0/identifying-political-bot-troll-social-media-activity-using-machine-learning-20dcd56e961a>.

174. For instance, one such takedown of inauthentic behavior on Facebook was accompanied by an announcement that identified only a small number of the 652 pages, groups, and accounts that were removed. See *Taking down More Coordinated Inauthentic Behavior*, FACEBOOK NEWSROOM (Aug. 21, 2018), https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/?wpisrc=NL_cybersecurity202&wpmm=1 [hereinafter *Taking Down*].

175. See *Indictment Underscores How Social Media Firms Got Played by Russian Agents*, CBS NEWS (Feb. 17, 2018, 7:33 AM), <https://www.cbsnews.com/news/indictment-underscores-how-social-media-firms-got-played-by-russian-agents/>.

176. See Douek, *supra* note 85, at 24.

C. Excluding U.S. Persons from FARA Registration

While the exact contours of the principal-agent distinction do not matter much when both parties are acting from abroad, the distinction becomes very relevant when considering U.S. citizen actors who are unwittingly involved with or unintentionally support foreign influence campaigns. As the District of Columbia Circuit noted, “Congress was particularly concerned that registration would not be imposed to stifle internal debate on political issues by citizens sympathetic to the views of foreigners but free from foreign direction or control.”¹⁷⁷ The case described above of Lee Stranahan, who works for Sputnik but claims that his pro-Russian positions are his own,¹⁷⁸ suggests the existence of a category of Americans who may echo the views of foreign propaganda operatives but are not acting as their witting agents. Additionally, there may be Americans whose social media accounts have been coopted by foreigner operatives: consider Rachel Usedom, a young American engineer in California, whose Twitter account was commandeered by propagandists.¹⁷⁹ There have also been a number of Americans who participated in rallies and other public protest events at the request of foreign-organized social media pages, falsely believing that they were authentic American pages.¹⁸⁰

All these U.S. persons would not be considered foreign agents under any definition in the Act. Under the Third Circuit’s agency test, a court would likely not find “consent” to have been granted when the agent is duped by a principal who fails to disclose his or her actual agenda. Under the Second Circuit’s “surrounding circumstances” test, the very nature of the relationship—a contact that the U.S. person involved believed to be purely innocent—suggests that the U.S. person did not know the shadowy motives behind the other side of the computer screen. As such, under either definition, FARA would not, under any interpretation, cover a U.S. person acting as an unwitting agent of a foreign principal. Recognizing the chance that such U.S. persons might get caught up in a foreign disinformation campaign, social media companies like Facebook have enacted procedures, such as passing posts flagged as potentially false to independent fact-checkers to

177. Attorney Gen. of U.S. v. Irish People, Inc., 796 F.2d 520, 524 (D.C. Cir. 1986).

178. See Gray, *supra* notes 114–15.

179. See Shane, *supra* note 119 (reporting that Usedom had tweeted up until 2014, but in November 2016 her account had been renamed “#ClintonCorruption” and was used to promote hacked material leaked by Russians without her knowledge).

180. See *supra* text accompanying note 96.

review before demoting them, to establish with greater certainty that the posts are not U.S. persons' independently posted content.¹⁸¹

D. Social Media Posts as Informational Materials

FARA, in its current form, requires filing and labeling “informational materials” in the following situation:

It shall be unlawful for any person within the United States who is an agent of a foreign principal and required to register under the provisions of this subchapter to transmit or cause to be transmitted in the United States mails or by any means or instrumentality of interstate or foreign commerce any informational materials for or in the interests of such foreign principal without placing in such informational materials a conspicuous statement that the materials are distributed by the agent on behalf of the foreign principal, and that additional information is on file with the Department of Justice, Washington, District of Columbia. The Attorney General may by rule define what constitutes a conspicuous statement for the purposes of this subsection.¹⁸²

If FARA were to apply to foreign-based social media propagandists, this section of the Act would suggest that these propagandists must also label and file their “informational materials” within forty-eight hours of their transmission.¹⁸³ The current definition of “informational materials” in the Act requires only that they be “for or in the interests of such foreign principal,” and can be “in any form which is reasonably adapted to being . . . disseminated or circulated among two or more persons.”¹⁸⁴ The Act does not give further meaning to the phrase “disseminated or circulated,” making it entirely possible to apply these terms to materials that are disseminated online as well.¹⁸⁵ But of course, rather than printing and distributing materials, today's social media propagandists rely almost exclusively on material shared over the Internet.¹⁸⁶ The nature of these materials impacts the breadth of their reach: whereas pamphlets had to be printed one at a time, bots can send out thousands of posts within seconds.¹⁸⁷ As such, while the language in FARA itself is capable of encompassing materials posted

181. See Mark Zuckerberg, *Preparing for Elections*, FACEBOOK (Sept. 12, 2018), <https://www.facebook.com/notes/mark-zuckerberg/preparing-for-elections/10156300047606634/>.

182. 22 U.S.C. § 614(b) (2012).

183. *Id.* § 614(a).

184. *Id.*

185. See *id.*

186. See generally Williams, *supra* note 170.

187. *Id.*

and distributed online, there are a few complications that arise when it comes to labeling online propaganda generally.¹⁸⁸

First, which part of a social media post should be labeled: the account page or each individual post? The DOJ FARA Unit staff has argued that it is impossible to require a label on each post,¹⁸⁹ and Senator Shaheen (D-NH) introduced a bill in 2017 proposing a scheme where foreign agents “may omit disclosure required . . . in individual messages, posts, or transmissions on social media on behalf of a foreign principal if the social media account or profile from which the information is sent includes a conspicuous statement” that the account is operating on a foreign entity’s behalf and that further information is on file with DOJ.¹⁹⁰ But if only the account page itself is identified, as Senator Shaheen has suggested, most Americans who view the account’s postings but not the account page itself are not likely to know that the account has been labeled as a foreign entity’s material. Alternatively, a verification mark, such as the one Twitter uses for all accounts of public interest, could help solve this problem.¹⁹¹ A “conspicuous statement” could be placed on the account page itself, but a FARA-specific verification mark would likely suffice to identify particular postings as related to a FARA-labeled account.

Second, the FARA Unit staff has pointed to a problem owing to the speed at which informational materials are posted online. DOJ has found that technological advances have made the forty-eight hour rule in the statute outdated, since registered agents now send out informational material on social media on a nearly continuous basis, making such a requirement unrealistic.¹⁹² Introduced legislation attempts to deal with this issue by removing the forty-eight hour requirement and replacing it with a requirement for filing at the same time and at the

188. Another aspect of this problem—that these online propagandists want to remain anonymous and are not inclined to label their own propaganda—will be tackled in the next Section.

189. See OFFICE OF THE INSPECTOR GEN., *supra* note 31, at 20.

190. S. 625, 115th Cong. § 3(b)(2)(B) (2017); see also *General FARA Frequently Asked Questions*, U.S. DEP’T OF JUSTICE, <https://www.fara.gov/fara-faq.html#1> (last visited Mar. 12, 2019) (suggesting that the FARA Unit has already adopted this recommendation). For other DOJ interpretations of the labeling requirement, for example with regard to mainstreaming the labeling of films, see *Keene v. Smith*, 569 F. Supp. 1513, 1516 (E.D. Cal. 1983).

191. See *generally About Verified Accounts*, TWITTER HELP CTR., <https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts> (last visited Mar. 12, 2019).

192. See OFFICE OF THE INSPECTOR GEN., *supra* note 31, at 19.

R

R

same intervals as an agent files their registration materials.¹⁹³ Yet if an account page itself is labeled under FARA, the issue largely resolves itself: technologically, a FARA-identifying verification mark can easily be automatically applied to each new posting from the already-labeled account.

The most challenging issue when it comes to labeling social media accounts is determining which accounts to label. While social media companies and the U.S. government, as discussed above, have identified the IRA as one specific actor in the Russian disinformation campaign, the identification of a specific organization with such certainty may not always be possible.¹⁹⁴ Perhaps, when there are multiple factors pointing to a determination that an account is being controlled by disinformation propagandists, that could be deemed sufficient to trigger the labeling requirement to make readers aware of such a determination. Unlike the current FARA registration system, where agents are registered in relation to specifically identified foreign principals, social media accounts need not be labeled with such specificity so long as an assessment is made that the account is reasonably believed to be of foreign origin.¹⁹⁵

When it comes to propaganda on social media, the concern is less the precise national identity of the propagandist than the fact that the propagandist is not a U.S. person. If such an approach is taken, the FARA label's text on the account page could be adapted from the current language. Rather than labeling informational materials as DOJ currently suggests ("this material is distributed by (name of registrant) on behalf of (name of foreign principal)"), in cases where the government is uncertain of the suspected foreign account's exact origin, FARA could require a label that reads, "This account has been flagged by the Department of Justice as material suspected of being distributed by a foreign entity to influence American political opinion."

Labeling accounts in this way would come with risks, chief among them the possibility that the account labeled later turns out to

193. S. 625 § 3(b)(1)(B).

194. *See supra* text accompanying note 174–76.

195. Note that it may be possible under the current terms of the Act to label the informational materials of actors that have not registered as foreign agents. Under the Act in its current form, the Attorney General is granted the authority to exempt certain agents from the requirement of furnishing any information otherwise required by FARA "where by reason of the nature of the functions or activities of such person the Attorney General, having due regard for the national security and the public interest, determines that such registration, or the furnishing of such information, as the case may be, is not necessary to carry out the purpose of this subchapter." 22 U.S.C. § 612(f) (2012).

be an account unaffiliated with any foreign propaganda campaign. To account for this possibility, FARA could grant the suspected foreign actor a period, such as ten days, during which the actor could reply with exculpatory evidence. The Act could also include a cause of action against the government available for people wrongly identified. In these circumstances, the FARA Unit could consider replacing the prior label it had placed on the account with one noting that the government has now confirmed that the account is operated by a U.S. person or a legitimate foreign independent actor.

Still, such an approach would be an uneasy solution. A scheme that involves labeling some accounts that may later prove innocent comes with potential legal challenges, such as arguments that the scheme is overbroad under the First Amendment, is a violation of the Due Process Clause of the Fourteenth Amendment, or entails labeling decisions that are arbitrary and capricious under the Administrative Procedure Act.¹⁹⁶ To protect against these and a flood of other possible challenges, any FARA enforcement regime would have to maintain a clear and consistent threshold in making determinations about which social media accounts should be labeled. To support this effort, the government could consider involving a third-party objective panel to make the FARA labeling determinations.¹⁹⁷

One such model currently exists regarding the Uniform Domain-Name Dispute Resolution Policy, where all domain name registration disputes are addressed using a third-party proceeding administered by ICANN, the nonprofit organization responsible for ensuring the stability of Internet network operations.¹⁹⁸ Another current model is the DMCA takedown notice, providing a web-based copyright dispute resolution system.¹⁹⁹ Under such an adjudicatory mechanism, as discussed above, users can be provided with a notice period during which they can submit exculpatory evidence to avoid labeling, thereby granting suspected disinformation users a means of redress. Nonetheless, whether a third-party panel could even make consistent attribution de-

196. See 5 U.S.C. § 706(2)(A).

197. Consider the independent third-party “Supreme Court” that Facebook has introduced to review its internal decisions on content moderation. See Sam Schechner & Kimberly Chin, *Facebook Opens New Fronts to Combat Political Interference*, WALL STREET J. (Jan. 28, 2019, 5:07 PM), <https://www.wsj.com/articles/facebook-vows-to-fight-election-interference-the-spread-of-fake-news-11548680757>.

198. See *Uniform Domain-Name Dispute Resolution Policy*, ICANN, <https://www.icann.org/resources/pages/help/dndr/udrp-en> (last visited Mar. 12, 2019).

199. See Rick Chapo, *DMCA Takedown Notice*, DMCA AGENT SERV. (July 18, 2016), <https://www.dmcaagentservice.com/dmca-takedown-notice/>.

terminations to some degree of certainty to begin with remains an open question.

E. Enforcing FARA in the Digital Age

While a 2016 Inspector General's report publicized DOJ's weak record of FARA enforcement in the early 2000s and 2010s,²⁰⁰ in the past couple of years FARA enforcement has become an essential part of DOJ's efforts to counter foreign influence operations in the United States.²⁰¹ There are also burgeoning efforts to give FARA enforcement more teeth. Until this past year, DOJ had not used its authority to seek civil injunctive relief in the form of a court order mandating registration since 1991.²⁰² Legislative efforts, such as the Disclosing Foreign Influence Act, are attempting to give DOJ the civil investigative authority to compel documentation,²⁰³ but these efforts are of limited effect when it comes to registering foreign social media propagandists. Even if such actors are identified with a certain degree of confidence, the agencies and organizations operating bot and troll accounts, which use fake identities and operate with the intention of staying anonymous, will certainly not volunteer for FARA registration. If compelled by a court, organizations such as the IRA will simply shut down an identified fake account and immediately open up a new one.²⁰⁴

This enforcement problem should be considered in two parts: (1) registration under the Act and (2) the labeling of informational materials. Regarding registration, DOJ does not have jurisdiction to compel a foreign entity to submit its paperwork under FARA.²⁰⁵ It cannot compel social media companies to refuse to publish the materials of suspected agents of foreign principals because FARA does not involve censoring materials.²⁰⁶ One possible effort at registration could be a

200. See generally OFFICE OF THE INSPECTOR GEN., *supra* note 31.

201. See Laufman, *supra* note 4.

202. *Id.* (noting that DOJ recently signaled its willingness to deploy this authority in its settlement agreement with Skadden, Arps, Slate, Meagher & Flom LLP, which was found to violate FARA).

203. See S. 2039, 115th Cong. § 12 (2017); H.R. 4170, 115th Cong. § 12 (2017); see also Foreign Agents Registration Amendments Act of 2018, S. 2483, 115th Cong. (2018).

204. See Matt O'Brien & Ryan Nakashima, *Social Media Plays Whack-a-Mole with Russia Interference*, AP NEWS (Aug. 1, 2018), <https://www.apnews.com/4ef29deb4a2d410ea1ba7d381a7d41b0>.

205. See Paul Rosenzweig, *Mueller's Message to America*, ATLANTIC (Feb. 17, 2018), https://www.theatlantic.com/politics/archive/2018/02/muellers-message-to-america/553658/?utm_source@ltw.

206. See *supra* text accompanying note 21.

naming and shaming operation, where the government releases a list of suspected foreign social media operatives and publicly puts these entities on notice that it intends to build a case against those who do not register voluntarily or provide exculpatory evidence within a given time period. While such a campaign would signal to these actors that the U.S. government has identified or is in the process of identifying them, it would still be toothless with regards to enforcement.²⁰⁷ Further, it could have the perverse outcome of causing the foreign actor to take down the suspected pages and create new ones.²⁰⁸

When it comes to the labeling requirement, it must be recognized that the social media companies often take down material posted by inauthentic accounts when they are able to identify them as such.²⁰⁹ However, there are many ways in which inauthentic accounts can get around social media companies' terms of service. On Twitter, for instance, there is no requirement that an account reveals the operator's true identity, so operating a fake account is not in and of itself a violation subject to takedown.²¹⁰ Therefore, posts that are not inflammatory—i.e., that do not incite hate speech or violence—and are deployed by trolls using their real names, may get flagged but would still remain online.²¹¹ While Facebook does ban coordinated inauthentic behavior completely,²¹² Facebook's official platform requires only

207. See Josephine Wolff, *What Good Is an Indictment for Online Election Meddling?*, SLATE (Feb. 16, 2018), <https://slate.com/technology/2018/02/the-russians-indicted-for-election-meddling-will-never-face-consequences.html>.

208. See generally *Taking Down*, *supra* note 174.

209. See Gold, *supra* note 115. But see Nicholas Confessore & Gabriel J.X. Dance, *On Social Media, Law Enforcement Lets Impostor Accounts Thrive*, N.Y. TIMES (Feb. 20, 2018), <https://www.nytimes.com/2018/02/20/technology/social-media-impostor-accounts.html> (reporting that social media companies often do not take down materials that violate their terms of service).

210. See Douek, *supra* note 85, at 29. Note, however, that Twitter has taken a number of steps to improve the security of its site, such as requiring purchasers of ads that advocate on “legislative issues of national importance” to verify their identities. See Tony Romm, *Twitter Will Begin Labeling Political Ads About Issues Such as Immigration*, WASH. POST (Aug. 30, 2018), <https://www.washingtonpost.com/technology/2018/08/30/twitter-will-begin-labeling-political-ads-about-issues-like-immigration/>.

211. See Issie Lapowsky, *Eight Revealing Moments from the Second Day of Russia Hearings*, WIRED (Nov. 1, 2017), <https://www.wired.com/story/six-revealing-moments-from-the-second-day-of-russia-hearings/>; see also Josh Constine, *The Trouble with Sandberg Saying Facebook Allows Fake News Ads*, TECHCRUNCH (Oct. 12, 2017), <https://techcrunch.com/2017/10/12/facebook-allows-fake-news/>.

212. See *Community Standards: 18. Misrepresentation*, FACEBOOK, <https://www.facebook.com/communitystandards/misrepresentation> (last visited Sept. 25, 2019). Note, however, that there is reason to suspect that fake pages go up on Facebook quicker than Facebook is able to take them down. See Siva Vaidhyanathan, *Why Facebook Will Never Be Free of Fakes*, N.Y. TIMES (Sept. 5, 2018), <https://www.nytimes.com/2018/09/05/opinion/facebook-sandberg-congress.html>.

R

R

the reduction, not removal, of false information, allowing some of these sources to remain online even if they have been identified as potentially fake.²¹³ Facebook also has suggested that unless there is a pressing political real-world event that fake news on its site is attempting to influence, it may choose not to take down suspected fake accounts so quickly.²¹⁴

Beyond the technical question of whether foreign propaganda always violates these platforms' terms of service, there are investigative, financial, and reputational considerations at play when it comes to issues of takedown and removal. Discussing the removal of fake accounts, Facebook has stated that "[i]f we remove them too early, it's harder to understand their playbook and the extent of their network."²¹⁵ This is because it sometimes takes less time to identify that a post violates a platform's policies than it does to identify the disinformation's source.²¹⁶ As these takedowns continue, the platforms may also eventually determine that removing suspected false accounts is unsustainable because of the harm such takedowns cause to user growth,²¹⁷ and the reputational damage caused by growing criticisms of arbitrary decision-making and political censorship.²¹⁸ Social media companies may also come to fear administrative actions taken by foreign countries in response to their takedown of suspected accounts.²¹⁹ As such, numerous cases may arise where a social media platform

213. See *Community Standards: 19. False News*, FACEBOOK, https://www.facebook.com/communitystandards/integrity_authenticity/false_news/ (last visited Sept. 25, 2019).

214. *Removing Bad Actors on Facebook*, *supra* note 122 (suggesting that Facebook took down certain accounts in the summer of 2018 because of "the connection between these bad actors and protests that are planned in Washington next week.") (last visited Sept. 25, 2019).

215. *Taking Down*, *supra* note 174.

216. See *Removing Bad Actors on Facebook*, *supra* note 122.

217. See Craig Timberg & Elizabeth Dwoskin, *Twitter is Sweeping Out Fake Accounts like Never Before, Putting User Growth at Risk*, WASH. POST (July 6, 2018), <https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/>.

218. See Elizabeth Dwoskin & Tony Romm, *Facebook Purged over 800 U.S. Accounts and Pages for Pushing Political Spam*, WASH. POST (Oct. 11, 2018), <https://www.washingtonpost.com/technology/2018/10/11/facebook-purged-over-accounts-pages-pushing-political-messages-profit/>.

219. See Ann M. Simmons, *Russia Accuses Facebook, Twitter of Failing to Comply with Data Laws*, WALL STREET J. (Jan. 21, 2019, 1:36 PM), <https://www.wsj.com/articles/russia-accuses-facebook-twitter-of-failing-to-comply-with-data-laws-11548085132>.

R

R

R

identifies a suspected fake account of foreign origin but is less inclined to immediately remove the account.²²⁰

In some of these instances—aside from cases where a platform chooses not to flag an account in an effort to continue to reap intelligence on the account’s origins by monitoring its continued activity—a case could be made for labeling these online “informational materials.”

Unlike traditional propagandists, social media propagandists such as the IRA will face no penalty if they flout requirements to label their pages under FARA. But the social media platforms on which these foreign-based social media propagandists disseminate their materials can, by contrast, be required to label these materials, or be voluntarily asked to do so.²²¹ While DOJ reports that it works closely with other government agencies in identifying potential FARA violators,²²² opportunities may exist for a more intensive collaboration in which the government and the social media platforms identify suspected foreign propagandists and label these accounts’ informational materials in real time. Indeed, such a model may be close to reality. Reports suggest that since at least mid-2018, the FBI and other federal agencies have been supplying intelligence that has helped social media platforms discover online disinformation actors,²²³ and the social media platforms have in turn shared their own findings with U.S. law enforcement.²²⁴ If greater efforts are made to label content in real time, it is also not implausible that bot and troll operators will come to view their activi-

220. The notion that social media companies are not taking down all suspected foreign disinformation actors is supported by the fact that Facebook removed only thirty-six accounts, six pages, and ninety-nine Instagram accounts ahead of the midterm elections. See Jessica Guynn, *Facebook: Fake Instagram Accounts Used Trump, Kanye and Social Issues to Target Voters*, USA TODAY (Nov. 13, 2018, 4:45 PM), <https://www.usatoday.com/story/news/2018/11/13/election-2018-results-how-russians-used-celebrities-target-voters/1991065002/>.

221. Requiring social media companies to take a more active role in FARA registrations would not be without precedent. See Joshua Geltzer, *A Checklist for Protecting Our Elections from Foreign Meddling*, JUST SECURITY (Jan. 12, 2018), <https://www.justsecurity.org/50948/checklist-protecting-elections-foreign-meddling/> (analogizing requiring more of the social media companies in this space to the reporting requirements imposed on financial institutions under the Bank Secrecy Act of 1970).

222. See U.S. DEP’T OF JUSTICE, *supra* note 36.

223. See Craig Timberland et al., *Tech Firms Step Up to Confront Online Threats. But Some Ask, What About the White House?*, WASH. POST (Aug. 24, 2018), <https://www.washingtonpost.com/technology/2018/08/24/tech-firms-step-up-confront-online-threats-some-ask-what-about-white-house/>.

224. See *Removing Bad Actors on Facebook*, *supra* note 146. When Facebook identified a number of accounts that violated its ban on coordinated inauthentic behavior in July 2018, its head of cybersecurity reported that the information had been shared with U.S. law enforcement agencies before it was removed. *Id.*

R

R

ties as a waste of time and energy, and slow down their creation of new accounts.

Suggestions of possible social media company liability frequently raise legal questions based on § 230 of the Communications Decency Act, which provides interactive computer services that include, for example, Facebook and Twitter, with civil immunity relating to any action undertaken to restrict access or availability of material on their platforms.²²⁵ However, § 230's policy goals include ensuring "vigorous enforcement of Federal criminal laws,"²²⁶ and § 230 specifically states that it does not impair the enforcement of any federal criminal statute.²²⁷ While the question of whether the government can enforce its criminal statutes without violating § 230 has not been extensively litigated, it is plausible that § 230 would not bar DOJ from holding social media companies liable under FARA for failing to label accounts that the government identifies—with the social media company's help—to be related to propagandist foreign entities.²²⁸ Additionally, recent movement in Congress in the area of sex trafficking online suggests the legislature's intent to allow for criminal enforcement and even civil suit against technology companies in some extreme cases.²²⁹ In congressional testimony in the fall of 2018, Twitter CEO Jack Dorsey said he was "open to dialogue" about § 230.²³⁰

225. See 47 U.S.C. § 230 (2012).

226. *Id.* § 230(b)(5).

227. See *id.* § 230(e)(1).

228. Note that social media companies such as Facebook and Twitter would not fall under FARA's news exception because, as indicated by their own words, they do not consider themselves news organizations but rather neutral technology platforms. See, e.g., Douek, *supra* note 48.

229. See Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018) (amending the Communications Decency Act to give prosecutors and sex trafficking victims alike a clearer route to pursue legal action against websites hosting advertisements for prostitutes). For a model of how liability could work for social media companies who knowingly maintain fake accounts or false information on their platform, consider the "knowledge" requirement in child pornography statutes. See generally Note, *Child Pornography, the Internet, and the Challenge of Updating Statutory Terms*, 122 HARV. L. REV. 2206 (2009). If this movement continues, it also may no longer be inconceivable to allow individuals to bring private suits against social media platforms if their material is wrongly labeled. For an example of a suit against a social media company for false labeling, see Bonnie Eslinger, *Facebook Censoring Russian Site by Deleting Page, Suit Says*, LAW360 (Nov. 20, 2018, 11:16 PM), <https://www.law360.com/cybersecurity-privacy/articles/1104112/facebook-censoring-russian-site-by-deleting-page-suit-says> (discussing the case of "[a] Russia-based website [that] sued Facebook in California federal court, claiming it is a legitimate news agency wrongly caught in the social media giant's fake news net").

230. Douek, *supra* note 48.

R

R

At the very least, enforcement of FARA with regards to social media companies appears increasingly plausible.

Requiring social media companies to label the informational materials of foreign operatives also raises a potential First Amendment challenge. The Supreme Court has held that an individual or group is not required to foster, display, or help promote those ideas with which the individual or group disagrees.²³¹ As such, social media companies may argue that the government is constitutionally barred from requiring them to include labels on certain accounts on their platforms. This pitfall suggests that a model of voluntary compliance with the government when it comes to FARA labeling would be more agreeable than a model of liability.²³² The government could even provide social media platforms with a safe harbor, such as absolute immunity, if they work voluntarily with DOJ in pursuing these labels.

Voluntary cooperation would not be without precedent; consider, for example, the Obama Administration's Countering Violent Extremism initiative, which sought to involve similarly close coordination between the government and the tech sector.²³³ Furthermore, legislative achievements such as the Cybersecurity Information Sharing Act ("CISA") have been premised on the very idea that improving cybersecurity requires the effective sharing of information between technology companies and the government.²³⁴ Any information sharing

231. See, e.g., *Pac. Gas & Elec. Co. v. Pub. Util. Comm'n of Cal.*, 475 U.S. 1, 25 (1986) (finding a First Amendment violation where Pacific Gas and Electric was required to include in its billing envelopes speech of a third party with which the company disagrees); *Wooley v. Maynard*, 430 U.S. 705, 717 (1977) (holding unconstitutional the requirement that motor vehicles bear license plates with the state motto 'Live Free or Die' on the grounds that the government could not compel an individual to display a message which fostered public adherence to a view which the individual disagreed with).

232. Reporting suggests that some voluntary social media giant-government cooperation is already underway: before the 2018 midterms, Facebook publicly acknowledged for the first time that the accounts it removed "were identified following a tip from law enforcement agencies." See Sheera Frenkel & Mike Isaac, *Russian Trolls Were at It Again Before Midterms, Facebook Says*, N.Y. TIMES (Nov. 7, 2018), <https://www.nytimes.com/2018/11/07/technology/facebook-russia-midterms.html>. Such cooperation is happening between social media companies and other governments around the world as well. See Sara Germano, *Facebook, Germany to Collaborate Against Election Interference*, WALL STREET J. (Jan. 20, 2019, 12:23 PM), <https://www.wsj.com/articles/facebook-germany-to-collaborate-against-election-interference-11548004995>

233. See Lisa O. Monaco, *How We're Countering Violent Extremism at Home and Abroad*, WHITE HOUSE: PRESIDENT BARACK OBAMA (Jan. 8, 2016, 4:10 PM), <https://obamawhitehouse.archives.gov/blog/2016/01/08/how-were-countering-violent-extremism-home-and-abroad>.

234. See generally Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (Supp. V 2018).

arrangement between DOJ and social media companies would have to be crafted in line with provisions in CISA, the Stored Communications Act (“SCA”), and other laws that limit private companies’ voluntary disclosure of personal user information to the government.²³⁵

F. Policy Considerations for the Tech Community

In the months immediately following the 2016 election, social media companies were reluctant to admit and respond to the extent of inauthentic activity on their platforms.²³⁶ Since then, the companies have accepted more responsibility. Facebook now has a team of over 20,000 people dedicated to safety and security, working to detect fake accounts using artificial intelligence before they are even created.²³⁷ Twitter has begun to emphasize the safety of its users over promoting public discourse at all costs, and has taken down millions of fake and suspicious accounts.²³⁸ The companies have also made progress with their terms of service. Among other reforms, Facebook has expanded its requirement that only authorized advertisers will be able to run “electoral” ads to political “issue” ads as well, and requires the verification of people who manage pages with large numbers of followers.²³⁹ Facebook also banned false information about voting requirements ahead of the 2018 elections.²⁴⁰ Twitter requires that “those running political ads for federal elections . . . identify themselves and certify that they are in the United States.”²⁴¹

These changes have not all been successful. For instance, Facebook’s attempt in 2018 to put red flags on fake news stories

235. See Timberland et al., *supra* note 223; see also Stored Communications Act, 18 U.S.C. § 2702 (2012); 6 U.S.C. §§ 1501–1506. R

236. See Aarti Shahani, *Zuckerberg Denies Fake News on Facebook Had Impact on the Election*, NPR (Nov. 11, 2016, 4:45 PM), <https://www.npr.org/sections/alltech-considered/2016/11/11/501743684/zuckerberg-denies-fake-news-on-facebook-had-impact-on-the-election>.

237. See *Taking Down Coordinated Inauthentic Behavior from Iran*, FACEBOOK NEWSROOM (Oct. 26, 2018), <https://newsroom.fb.com/news/2018/10/coordinated-in-authentic-behavior-takedown/>.

238. See Timberg & Dwoskin, *supra* note 217. R

239. See Rob Goldman & Alex Himel, *Making Ads and Pages More Transparent*, FACEBOOK NEWSROOM (Apr. 6, 2018), <https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/>. Facebook has also developed a searchable database of political ads, which it has expanded around the world. See Schechner & Chin, *supra* note 197. R

240. See Joseph Menn, *Exclusive: Facebook to Ban Misinformation on Voting in Upcoming U.S. Elections*, REUTERS (Oct. 15, 2018), <https://www.reuters.com/article/us-facebook-election-exclusive/exclusive-facebook-to-ban-misinformation-on-voting-in-upcoming-u-s-elections-idUSKCN1MP2G9>.

241. See Nellie Bowles & Sheera Frenkel, *Facebook and Twitter Plan New Ways to Regulate Political Ads*, N.Y. TIMES (May 24, 2018), <https://www.nytimes.com/2018/05/24/technology/twitter-political-ad-restrictions.html>.

backfired when users began sharing the labeled hoaxes even more,²⁴² and Facebook’s introduction of a “tool that verifies ad-buyers’ identities . . . still allows ads from buyers with falsified identities to slip through.”²⁴³ Twitter’s efforts to combat tweets that most likely come from bad actors have often only pushed the tweets down into the “show more replies” section, rather than labeling the tweets as fake.²⁴⁴ The same group of Internet trolls that meddled in the 2016 political process tried to influence American voters using Facebook ahead of the midterm elections, suggesting that despite Facebook’s efforts, it continues to be a battleground for disinformation actors.²⁴⁵ The social media companies have also been criticized for selective as well as overbroad enforcement in their removal of suspicious accounts.²⁴⁶

In light of the continuing challenges that social media companies face when it comes to self-regulating foreign social media propagandists, appetite remains for congressional action. In September 2018, Senator Mark Warner, Vice Chairman of the Senate Intelligence Committee, stated that “Congress is going to have to act. . . . The era of the Wild West of social media is coming to an end.”²⁴⁷ Whether Congress chooses to regulate social media companies on this issue through FARA, the Honest Ads Act, or other pending legislative proposals is not for this Article to determine. But if Congress does choose to regulate in this space either through FARA or through another law, a number of broad principles, outlined below, could play an important role in alleviating the regulatory concerns of the social media companies at issue.

First, Congress must carefully consider the scope of any regulatory solution. It may not make regulatory sense to require every social media startup, for instance, to identify and label the foreign-based propaganda on its platform. As is well-evident, the kind of propaganda discussed in this Article is only a national concern when it is distrib-

242. See Constine, *supra* note 211.

R

243. Caitlin Fairchild, *Senators Want Facebook to Fix Ad Transparency Tool*, NEXTGOV (Nov. 5, 2018), <https://www.nextgov.com/emerging-tech/2018/11/senators-want-facebook-fix-ad-transparency-tool/152574/> (revealing that an Iranian campaign was recently able to buy ads on Facebook and Instagram while using the revamped verification process).

244. See Lucas Matney, *Twitter Algorithm Changes Will Hide More Bad Tweets and Trolls*, TECHCRUNCH (May 15, 2018), <https://techcrunch.com/2018/05/15/twitter-algorithm-changes-will-hide-more-bad-tweets-and-trolls/>.

245. See Frenkel & Isaac, *supra* note 232.

R

246. See Cristiano Lima, *Facebook Removals Draw Mixed Reviews*, POLITICO (Oct. 12, 2018, 10:00 AM), <https://www.politico.com/newsletters/morning-tech/2018/10/12/facebook-removals-draw-mixed-reviews-372174>.

247. See Douek, *supra* note 48.

R

uted en masse. Therefore, similar to how federal discrimination laws apply differently to companies with fourteen or fewer employees,²⁴⁸ any regulation in this space could be limited to platforms that reach a threshold of a certain number of users. Congress could identify a number of concrete factors that determine whether a social media company has reached this threshold.

Second, any regulation would likely need to standardize the identification and labeling system that would be used across social media platforms so users can easily identify a labeled account and understand what the label means. Through organizations such as the National Institute for Standards and Technology, the government has experience tackling these sorts of collective action problems and could apply that experience to this issue as well.²⁴⁹ As discussed above, a universally recognizable FARA-specific verification mark could allow for easy identification of suspected accounts.

Finally, it may be important to keep in mind the international effects of any U.S. regulation: a strict enforcement regime could, theoretically, drive the business of emerging technology companies to other countries. As such, any regulatory regime in this space may ultimately be more effective if it is undertaken in coordination with foreign countries and partners, establishing uniform standards and requirements. Given that the United States is not the only country affected by disinformation campaigns,²⁵⁰ it is likely that other countries would be interested in identifying and putting into place shared approaches and standards.

CONCLUSION

If Congress decides to implement a FARA registration and labeling regime for foreign-based social media propagandists, it should not be under the illusion that doing so on its own would solve the disinformation problem. To a significant degree, the problem of fake news on social media often resembles a game of whack-a-mole, where a new account pops up for every account taken down.²⁵¹ It is probably

248. *FAQ #1: Do the Federal Employment Discrimination Laws Apply to My Business?*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/employers/smallbusiness/faq/do_laws_apply.cfm (last visited Mar. 12, 2019).

249. *See About Standards.gov*, NIST, <https://www.nist.gov/standardsgov/about-standardsgov> (last updated Aug. 8, 2018).

250. *See Yasmine Serhan, Italy Scrambles to Fight Misinformation Ahead of Its Elections*, ATLANTIC (Feb. 24, 2018), <https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/>.

251. *See Kevin Poulsen, Alleged Russian Operatives Spreading Fake News Sneak Back onto Facebook*, DAILY BEAST (Sept. 5, 2018, 5:14 AM), <https://www.thedaily>

better to institute a regulatory regime that tackles part of the problem rather than to not tackle the problem at all, and the institution of a regulatory regime may play a role in changing the dynamics of these disinformation campaigns. It remains an open question, however, whether FARA is the best tool to use.

This Article has identified how FARA can be applied statutorily to foreign-based social media actors, as well as the enforcement challenges that any such registration and labeling regime would face. In some ways, FARA is a good fit for this problem: trolls and bots are beginning to share, retweet, and otherwise engage with genuine, domestically produced content, rather than generating their own content. This suggests that FARA's emphasis on the *actor*, rather than the *content*, aligns with disinformation actors' present tactics.²⁵² But labeling suspected foreign accounts comes with numerous legal and technical challenges, as discussed above, indicating the difficulties of a label-based regulatory model.

Ultimately, the question of FARA's applicability to foreign-based social media actors is just one element of a policy conversation about how the United States might stay ahead of the problem of foreign disinformation on social media. Given the rapidly changing nature of technology, it is clear that none of the measures discussed here would serve as a comprehensive panacea for this problem. Nonetheless, it is important to look at individual laws like FARA that operate in this area, and to consider the opportunities and pitfalls behind expanding or applying any one of them to this novel and evolving threat.

beast.com/alleged-russian-operatives-spreading-fake-news-sneak-back-onto-facebook (reporting that two weeks after Facebook "expunged" a site linked to Russia, the banned site used a different Moscow publisher as a cut-out to put its content back onto the site). *But see* Timberg, *supra* note 10 (discussing a Knight Foundation report that suggests that fake news "isn't hundreds of accounts, and [fighting it] isn't Whack-a-mole and . . . It's a couple of dozen persistent sites that do this all day, every day").

252. *See* Cristiano Lima, *The Future of Russian Disinformation*, POLITICO (Dec. 18, 2018, 10:00 AM), <https://www.politico.com/newsletters/morning-tech/2018/12/18/the-future-of-russian-disinformation-459107> ("[I]nstead of generating their own content to inflame America's social and political divides, [trolls in 2020 will] likely share, retweet and otherwise engage with genuine, domestically produced content that aligns with those goals.").

