HOW FOREIGN STATES AND TERRORIST ORGANIZATIONS USE SOCIAL MEDIA TO UNDERMINE U.S. DEMOCRACY

Molly Magnis

I. INTRODUCTION

The use of social media has completely and forever changed human interaction. But while it may not be surprising to hear that social media has changed the way humans communicate with each other, the fact that social media is being used to negatively affect and undermine U.S. democracy may be less obvious. Social media is generally thought of as the means that allows people to instantly communicate with friends and family.[1] Since 1997, social media sites have allowed users to create a personal profile and become "friends" with other users, which then allows the friends to communicate with each other online.[2] Throughout the subsequent two decades, hundreds of social media websites were created and have been used to promote businesses, advertise products, share ideas, and of course, connect with people from around the world.[3]

Unfortunately, these connections are not always favorable. As this paper will discuss, popular social media sites such as Facebook, Twitter, and Google have confirmed that millions of site users were exposed to Russian-controlled accounts whose purpose was to spread disinformation about the 2016 U.S. Presidential Election in an effort to either influence the outcome of the election, or "discredit our democracy and divide [American citizens.]"[4]

---

[1] *See* Benjamin Hale, *The History of Social Media: Social Networking Evolution!*, HISTORY COOPERATIVE (June 16, 2015), https://historycooperative.org/the-history-of-social-media/.

[2] See *id.*

[3] *See id.*

[4] Hamza Shaban et al., *Facebook, Google and Twitter Testified on Capitol Hill. Here's What They Said.*, THE WASH. POST (Oct. 31, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/31/facebook-google-and-twitter-are-set-to-testify-on-capitol-hill-heres-what-to-expect/?utm_term=.80e404bbefa6.

Additionally, terrorist groups such as ISIS have used social media sites including Twitter, Facebook, and KIK to connect with teens and young adults in Western countries in an effort to recruit them and spread ISIS propaganda.[5] These efforts are part of ISIS' goal to destroy and terrorize those it believes to be "promoting democracy and 'ideas that distort[] Islam.'"[6] Senator Lindsey Graham of South Carolina stated that the "ability of terrorists to recruit followers over social media and foreign governments to meddle in American democracy" are the "national security challenge[s] of the 21st century."[7]

Efforts to combat these challenges, however, have caused numerous conflicts with U.S. laws and Constitutional rights, including the incredible protections afforded to free speech in the U.S.; the leniency that has been given to social media companies in laws such as the "small items" exception to the Federal Election Campaign Act and the Communications Decency Act Section 230(c)(1); court decisions in cases such as *Fields v. Twitter, Inc.*, 881 F.3d 739 (9th Cir. 2018), *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150 (N.D. Cal. 2017), and *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140 (E.D.N.Y. 2017); and the rejection of legislation such as H.R. 3654 Combat Terrorist Use of Social Media Act of 2015, S. 2517 Combat Terrorist Use of Social Media Act of 2016, and H.R. 4820 Combatting Terrorist Recruitment Act of 2016. This paper will explore how both Russian and ISIS national security threats affect U.S. democracy, and the steps that social media companies and the U.S. legislature have taken to combat such foreign threats.

II. RUSSIA

A. The Kremlin Playbook

After being used to successfully aid in the collapse of the Soviet Union,[8] Western democratic ideals are now being attacked by

---

[5] Hollie McKay, *'Jihadi Cool': How ISIS Switched its Recruitment and Social Media Master Plan*, FOX NEWS NETWORK (Apr. 3, 2017), http://www.foxnews.com/world/2017/04/03/jihadi-cool-how-isis-switched-its-recruitment-and-social-media-master-plan.html.

[6] Adam Withnall, *Isis's War on Democracy: Militants Execute 300 Civil Servants From Iraqi Electoral Commission*, THE INDEP. (Aug. 9, 2015), http://www.independent.co.uk/news/world/middle-east/isiss-war-on-democracy-militants-execute-300-civil-servants-from-iraqi-electoral-commission-10447519.html.

[7] Shaban et al., *supra* note 4.

[8] *See* Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian*

Russia in an attempt to dismantle Western democracies through the country's "war on information" campaign.[9] As explained in *The Kremlin Playbook,* the purpose of this campaign is to "confuse, paralyze, and disable [Russia's] opponents and obscure the truth. . . . " by spreading false and skewed information about its opponents' governments.[10] Instead of using force and violence, Russia uses the power of influence to "weaken[] the internal cohesion of societies and strengthen[] the perception of the dysfunction of the Western democratic and economic system. . . . "[11] Russia's ultimate goal is to polarize the citizens of Western democracies and convince them that their democratic system is inefficient, and that Russia's system of illiberal democracy is a more stable and desirable form of government.[12] While democracies in Western countries are generally categorized as liberal, an illiberal democracy is one that appears to hold democratic elections but bends the laws so those in power stay in power, while the citizens are deprived of their basic rights and civil liberties.[13] Currently, the Kremlin, (the Russian government), is seeking to spread illiberal democracy throughout Central and Eastern Europe and the United States through its "war on information."[14]

B. Using Social Media to Further Russia's "War on Information"

In 2009, Former U.S. President Barack Obama received a letter from leaders in Central and Eastern Europe warning that "Russia was conducting 'overt and covert means of economic warfare'" which included "media manipulation in order to advance [Russian] interests. . . . "[15] Since then, Russia has taken advantage of the inherent weaknesses in the United States' media and freedom of speech policies by providing false news stories to U.S. media

---

Influence in Central and Eastern Europe, CTR. FOR STRATEGIC AND INT'L STUD., 5 (Oct. 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf.

9 *Id.* at 6.

10 *Id.*

11 *Id.* at 5.

12 *See id.*

13 Dani Rodrik & Sharun Mukand, *Why Illiberal Democracies Are on the Rise*, HUFF POST, https://www.huffingtonpost.com/dani-rodrik/illiberal-democracies-on-the-rise_b_7302374.html (last updated May 17, 2016).

14 Conley et al., *supra* note 8 at 6.

15 *Id.* at IX.

outlets which then "disseminate erroneous information that fosters public confusion and disillusionment,"[16] especially through the fairly unrestricted platforms of social media.[17]

In recent months, social media sites such as Twitter and Facebook have discovered hundreds of Russian-linked accounts that have been used to spread politically polarizing information since before the 2016 U.S. Presidential election.[18] Along with Anti-American sentiments, some accounts spread false information regarding Hillary Clinton, including accusations that she funded violent, left-wing anti-fascist protesters.[19] Another Russian account falsely reported that President Donald Trump was endorsed by Pope Francis.[20] Yet another Russian account, operating under the name "Army of Jesus," called Clinton "a Satan" and encouraged people to vote for Donald Trump since he was an "honest man" who "cares deeply for this country."[21] This post included a picture in which Jesus, who supported Trump, and the devil, who supported Clinton, were arm wrestling and encouraged people to "PRESS 'LIKE' TO HELP JESUS WIN!"[22]

Experts on Russia say that Russian President Vladimir Putin "hoped to damage, if not defeat, Mrs. Clinton, whom he blamed for encouraging pro-democracy protests in Russia and neighboring states."[23] Despite this hope, the director of the Alliance for Securing Democracy, Laura Rosenberger, explained that a majority of the information spread by Russia on social media was not about a specific political candidate, but was meant to "creat[e] societal division, [by] identifying divisive issues and fanning the

---

16 *Id.* at XIV.

17 *See* Daisuke Wakabayashi & Scott Shane, *Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election*, N.Y. TIMES (Sept. 27, 2017), https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html.

18 *See id.*

19 *See id.*

20 *See* Craig Timberg & Elizabeth Dwoskin, *Russian Content on Facebook, Google and Twitter Reached Far More Users Than Companies First Disclosed, Congressional Testimony Says*, WASH. POST (Oct. 30, 2017), https://www.washingtonpost.com/business/technology/2017/10/30/4509587e-bd84-11e7-97d9-bdab5a0ab381_story.html?utm_term=.59df5952fb4d.

21 Amber Phillips, *Russia Tried to Corrupt the 2016 Election. Could it do the Same Tuesday?*, WASH. POST (Nov. 5, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/11/05/russia-tried-to-corrupt-the-2016-election-could-it-do-the-same-tuesday/?utm_term=.f60620046c6e.

22 *Id.*

23 Wakabayashi & Shane, *supra* note 17.

flames."[24] For example, Twitter accounts that have been linked to Russia were recently tweeting conflicting messages regarding Trump's position on NFL players who chose not to stand during the national anthem, by using "#standforouranthem" in some tweets, and "#takeaknee" in others.[25] This trend of conflicting messages was also found in over "3,000 Russian-linked [Facebook] advertisements" that included "issues such as religion, race, gun ownership," immigration, and other racial and political topics that have been at the core of American debates.[26]

These tweets and advertisements were far-reaching, as evidenced by Twitter's announcement in late October 2017 that 2,752 Twitter accounts were found to be controlled by Russia, and "more than 36,000 Russian bots tweeted 1.4 million times during the [2016 election]."[27] Additionally, Facebook announced that due to users sharing, "liking," and commenting on Russian posts, "as many as 126 million people may have seen material in their news feeds that originated from Russian operatives. . . . "[28] Facebook also found 470 Russian-linked accounts and pages that paid over $100,000 for the 3,000 advertisements found to be linked to Russia's "war on information."[29] Furthermore, Google reported finding 1,108 YouTube videos that contained 43 hours of content posted by Russian operatives, and $4,700 worth of Russian search and display advertisements – all of which had the purpose of influencing American voters during the 2016 election.[30]

C. Laws Combatting Foreign Influence on Domestic Elections

The Federal Election Commission (FEC), in the Federal Election Campaign Act, prohibits "foreign nationals" from making any contributions or donations to U.S. elections, including contributions to specific political parties or candidates.[31] Relatedly, the FEC requires political advertisements classified as

---

[24] *Id.*

[25] *Id.*

[26] Mike Isaac & Scott Shane, *Facebook to Deliver 3,000 Russia-Linked Ads to Congress on Monday*, N.Y. TIMES (Oct. 1, 2017), https://www.nytimes.com/2017/10/01/technology/facebook-russia-ads.html.

[27] Shaban et al., *supra* note 4.

[28] Timberg & Dwoskin, *supra* note 20.

[29] *Id.*

[30] *Id.*

[31] Myles Martin, *Foreign Nationals*, FEDERAL ELECTION COMMISSION (June 23, 2017), https://www.fec.gov/updates/foreign-nationals/.

"public communication" to contain a disclaimer that identifies the person or organization who paid for the ad, and who authorized the communication.[32] "Public communication" includes mediums such as television broadcasting, newspaper ads, mass mailings, and "other general public political advertising," but "does not include internet ads, except for communications placed for a fee on another person's web site[.]"[33]

While purchasing an advertisement on Facebook would technically qualify as a communication made on another's web site which requires a disclaimer, Facebook requested a "small items" exception from this rule in 2011, when it argued that the character limit restrictions of its ads made the disclaimers impractical.[34] Unlike radio stations, newspapers, and television companies, Twitter and Google adopted Facebook's argument and have likewise not been required to disclose the identity of those purchasing political advertisements on its sites.[35] Consequently, these exceptions to disclosure allowed Russia to purchase $100,000 worth of Facebook advertisements and $4,700 worth of advertisements on Google during the 2016 election while remaining anonymous to the average internet user.[36] While the company was not required to disclose the purchaser's identity, Facebook was highly criticized for "failing to discover the [illegal] Russian online influence campaign sooner, especially given that many of the [political] ads were paid for in rubles, the Russian currency."[37]

In response to these criticisms, Mark Zuckerberg, Facebook's chief executive, stated that he "care[d] deeply about the democratic process" and wanted to prevent anyone from using Facebook "to undermine democracy."[38] To support this statement, Zuckerberg

---

[32] FED. ELECTION COMM'N, SPECIAL NOTICES ON POLITICAL ADS AND SOLICITATIONS (2006), https://transition.fec.gov/pages/brochures/notices.shtml.

[33] *Id.*

[34] *See* Donie O'Sullivan, *Facebook Sought Exception from Political Ad Disclaimer Rules in 2011*, CNN (Sept. 27, 2017), http://money.cnn.com/2017/09/27/technology/business/facebook-political-ad-rules/index.html.

[35] *See* Isaac & Shane, *supra* note 26.

[36] *See* Kenneth P. Vogel & Cecilia King, *Senators Demand Online Ad Disclosures as Tech Lobby Mobilizes*, N.Y. TIMES (Oct. 19, 2017), https://www.nytimes.com/2017/10/19/us/politics/facebook-google-russia-meddling-disclosure.html.

[37] Shaban et al., *supra* note 4.

[38] Craig Timberg et al., *Facebook to Turn Over Thousands of Russian Ads to Congress, Reversing Decision*, WASH. POST (Sept. 21, 2017), https://www.washingtonpost.com/business/technology/facebook-to-turn-over-

announced in late September 2017 that Facebook would be increasing its security measures, and that each Facebook ad would now show who created and paid for the advertisement.[39] Google also announced that its site would be "creat[ing] a publicly accessible database of all election ads purchased on Google's ad platform and on YouTube," to create transparency by "identify[ing] the [ad] purchasers and how much money was spent."[40]

While these attempts to pre-empt legislative regulations and tighten the companies' own security is appreciated, some U.S. Senators have already supported a bill entitled the "Honest Ads Act" that "would require digital platforms with more than 50 million monthly viewers to create a public database of political ads purchased by a person or group who spends more than $500."[41] Unlike Google's plans for security though, this bill would require the following additional information to be disclosed in the public database: "the ad, a description of the targeted audience, the number of views [the ad] generated, the date and time it ran, its price[,] and contact information for the purchaser."[42] Despite Zuckerberg's statements in support of protecting the integrity of U.S. elections and the democratic process, as of late October 2017, neither Facebook nor Google agreed to support this bill.[43] Twitter, however, began adopting such additional safeguards on its own by requiring that all advertisements of state and federal political candidates be verified[44] in its new Advertising Transparency Center.[45] The Center will provide information about the ad's promoters and financers, as well as allow the users to see who the ad is targeting, why they are being targeted, and allow the user to tell Twitter they do not wish to see the ad.[46]

---

thousands-of-russian-ads-to-congress-reversing-decision/2017/09/21/9790b242-9f00-11e7-9083-fbfddf6804c2_story.html?utm_term=.2cfebde27d41.

39 *Id.*

40 Shaban et al., *supra* note 4.

41 *Id.*

42 *Id.*

43 *See id.*

44 *See* Hillary Grigonis, *Here's What Social Media Giants are Doing to Keep Extremism Off Your Screen*, DIGITAL TRENDS (Jan. 18, 2018), https://www.digitaltrends.com/social-media/senate-hearing-terrorism-and-social-media-extremist-content-january-2018/.

45 *See* Hillary Grigonis, *Twitter Isn't Waiting for New Laws Before Labeling Who Paid for Political Ads*, DIGITAL TRENDS (Oct. 25, 2017), https://www.digitaltrends.com/social-media/twitter-advertising-transparency-center/.

46 *See id.*

D. Why Do We Need More Internet Advertisement Regulations?

While the legislature is hoping to enact the Honest Ads Act, some are weary of having this problem fixed by political actors.[47] One source suggests that political "[r]egulatory bureaucrats" will do little to actually prevent this foreign influence on our democracy, since they generally benefit from the political divide.[48] This source provides an alternative to regulation, in which Americans would be taught to critically analyze the information they see online and be encouraged to investigate the underlying biases of the sources.[49] But would this method truly be effective? Is it practical to think that every social media user will take the time to investigate for themselves whether an online advertisement or news story is accurate, especially if it is in line with their own thoughts and beliefs?

E. Conclusion

In the Federalist Papers No. 68, Alexander Hamilton warned the States about the danger of foreign governments interfering with American elections,[50] by calling foreign governments "deadly adversaries of the republican government" who "desire . . . to gain an improper ascendant in our councils."[51] To combat this danger, Hamilton explained that "the convention" gave the American people the power to choose who their President would be rather than giving that power to "preexisting bodies of men, who might be tampered with beforehand to prostitute their votes[.]" [52] Hamilton's words provide insight as to how important it was to the Founders that the U.S. President be chosen by the American people and by no other organization, entity, or foreign government to ensure that our democracy was not corrupted.[53] If Russian operatives are now manipulating our election process by influencing American voters through social media, then the President of the United States is no longer being directly chosen

---

47 *See* Mark A. Jamison, *What the Facebook-Russian Nexus Can Teach Us*, REAL CLEAR POLITICS (Sept. 22, 2017), https://www.realclearpolitics.com/articles/2017/09/22/what_the_facebook-russian_nexus_can_teach_us_135069.html.

48 *Id.*

49 *Id.*

50 *See* Wakabayashi & Shane, *supra* note 17.

51 THE FEDERALIST NO. 68, at 352 (Alexander Hamilton).

52 *Id.* at 353.

53 *Id.* at 352–54.

by the people of the United States, which consequently deems our democratic system ineffective. To ensure that social media sites are following-through on efforts to ensure democratic integrity, the legislature must enact regulations that will expose the details of who is purchasing the political internet advertisements, to ensure that the American people have the ability to interpret the underlying message and credibility of the ads, and to prevent our country from being controlled by foreign actors that reject democracy.

III. ISIS

A. Terrorist Wars and Threats Against Democracy

Similar to Russia's attempt to divide American citizens and discredit U.S. democracy, one objective of the Islamic State of Iraq and Syria ("ISIS" or "the Islamic State")[54] is to create a division between the Muslim and non-Muslim members of Western democratic societies in an effort to draw all Muslims to its regime.[55] ISIS' ultimate goal is to create a global "caliphate" – an Islamic State governed by Sharia law and run by a "caliph" or successor of the Prophet Muhammad.[56] This system runs contrary to Western democracies, since democratic leaders are not chosen based on the successor of the Prophet Muhammad, but instead through a system of voting by the State's citizens.[57] ISIS refuses to recognize any system of government that is not controlled by Sharia law, and uses violence to acquire territory for its caliphate and destroy any "disbelievers"[58] – including those who promote democracy and "ideas that distort[] Islam."[59] ISIS also condemns "grayzones,"

---

[54] Helen Lock, *Isis vs Isil vs Islamic State: What Do They Mean – And Why Does it Matter?*, THE INDEP. (Sept. 14, 2014), http://www.independent.co.uk/news/world/middle-east/isis-vs-isil-vs-islamic-state-what-is-in-a-name-9731894.html.

[55] *See* Daniel Burke, *Why ISIS is Celebrating Trump's Immigration Ban*, CNN (Jan. 31, 2017), https://www.cnn.com/2017/01/31/us/islamerica-excerpt-grayzones/index.html.

[56] *See* Adam Chandler, *What is an Islamic Caliphate and Why Did ISIS Make One?*, THE ATLANTIC (June 30, 2014), https://www.theatlantic.com/international/archive/2014/06/what-is-an-islamic-caliphate-and-why-did-isis-make-one/373693/.

[57] *See* Tim Lister, *What Does ISIS Really Want?*, CNN (Dec. 11, 2015), https://www.cnn.com/2015/12/11/middleeast/isis-syria-iraq-caliphate/index.html.

[58] *Id.*

[59] Withnall, *supra* note 6.

("areas where Muslims practice their religion peacefully in non-Muslim countries"), since such areas are not governed by Sharia law.[60] In an effort to draw other Muslims out of "grayzones" and into its Islamic State, ISIS hopes that terrorist attacks in such non-Muslim countries will cause Westerners to alienate and marginalize Muslims, who will then believe that the West is anti-Islam and cause them to run "into the caliphate's open arms."[61]

B. Using Social Media to Further ISIS' War on Democracy

i. Recruiting Westerners to Syria

A more direct method of turning Muslims against Western democracies and recruiting them into the terrorist organization is through the use of social media.[62] ISIS has become the first terrorist group to successfully recruit thousands of people from around the world via social media websites such as Facebook, Twitter, Tumblr, YouTube, and Kik.[63] ISIS uses such sites to gain foreign followers and post ISIS propaganda videos that compel said followers to travel to ISIS territory.[64] The group then provides instructions and guidance to help the new recruits cross the border into Syria to join the caliphate.[65] In April 2015, *The New York Times* reported that "foreigners make up half of ISIS' fighting force, and an estimated 4,000 come from Western countries."[66] In September of 2015, the House Homeland Security Committee reported that about 250 Americans had traveled to Syria and Iraq to join ISIS,[67] with a majority of these Americans ranging from teenagers to early 20-year-olds.[68]

---

60 Burke, *supra* note 55.

61 *Id.*

62 *See* Pamela Engel, *ISIS has Mastered a Crucial Recruiting Tactic No Terrorist Group Has Ever Conquered*, BUS. INSIDER (May 9, 2015), http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5.

63 *See id.*

64 *See id.*

65 *See id.*

66 *Id.* (citing Mary Ann Weaver, *Her Majesty's Jihadists*, N.Y. TIMES (Apr. 14, 2015), https://www.nytimes.com/2015/04/19/magazine/her-majestys-jihadists.html).

67 *See* Dina Temple-Raston & Steve Inskeep, *Report: 250 Americans Have Gone to Syria and Iraq to Fight*, NPR.ORG (Sept. 29, 2015), https://www.npr.org/2015/09/29/444398846/report-250-americans-have-gone-to-syria-and-iraq-to-fight.

68 *See* Richard Engel et al., *The Americans: 15 Who Left the United States to*

In May 2016, NBC News reported about 15 such Americans who left the United States to join ISIS in its fight against democracy.[69] One boy, Hanad Abdullahi Mohallim, was 18-years-old when he entered Syria in March 2014.[70] Once in Syria, Mohallim communicated with his U.S. friends on Facebook, where he showed them pictures of himself holding guns and convinced them to also join him in Syria.[71] Another boy, Abdi Nur, was about 20-years-old when he entered Syria in November 2014.[72] After being indoctrinated himself via Facebook, Nur also used Facebook as a means to communicate with his U.S. friends, post pictures of himself holding guns, and attempted to convince his friends to join him and the caliphate.[73]

A third boy, Asher Abid Khan, was only 19-years-old when he was exposed to ISIS propaganda recruitment videos on YouTube that "encouraged Western Muslims to come to Syria and assist in the fight against the Assad regime, using the cause deceptively as a front to enlist in ISIS."[74] After travelling as far as Turkey, he changed his mind about joining ISIS and returned to the U.S. where he was charged with "conspiracy and attempting to provide material support to [a terrorist organization]."[75] The reasons for such interest in joining the organization have been discussed by many. Asher's defense attorney, Thomas Berg, stated that "[t]he ideas being sent out [by ISIS recruiters] are sophisticated in the sense that they portray a romantic ideal of something, in the nature of a religious obligation or duty in jihad."[76] Dr. John Horgan, "a forensic psychologist and expert in analyzing terrorist behavior," explained that teenagers are especially vulnerable to ISIS propaganda as they are searching for a purpose and place to fit in the world.[77] Organizational psychology consultant Zac

---

Join ISIS, NBC NEWS (May 16, 2016), https://www.nbcnews.com/storyline/isis-uncovered/americans-15-who-left-united-states-join-isis-n573611. *See also* Dorian Geiger, *This is How ISIS Uses Social Media to Recruit American Teens*, TEEN VOGUE (Nov. 20, 2015), https://www.teenvogue.com/story/isis-recruits-american-teens.

69 *See* Engel et al., *supra* note 68.

70 *Id.*

71 *Id.*

72 *Id.*

73 *Id.*

74 Geiger, *supra* note 68.

75 *Id.*

76 *Id.*

77 *Id.*

Parsons, whose focus is on online behavior, suggested that the promise of "doing God's work is very appealing" to teens, especially when they are promised a "paradise" when they become martyrs.[78]

ii. ISIS Recruits Remaining in the U.S. and Lone Wolf Attacks

After 2014 and 2015 brought a surge of Americans traveling to Syria to join ISIS, an increasing number of Western ISIS recruits began contacting their embassies in April 2016 expressing their desire to leave ISIS territory and return to their home countries.[79] While this may be attributed to ISIS' loss of territory and power (leading recruits to question their allegiance to the group), the chancellor of security for the Kurdistan Regional Government in northern Iraq, Masrour Barzani, warned that "the threat foreign fighters can still pose upon returning to their countries should not be underestimated,"[80] as many fear that their return may bring domestic attacks on their home countries.[81]

Relatedly, Americans have become increasingly concerned about ISIS recruits who become radicalized over the internet but then *remain* in the U.S.[82] This newer phenomenon involves exposing its followers to ISIS propaganda via social media – which includes photographs and videos of "beheadings and other atrocities, as well as audio and video lectures by members of ISIS. . . . " – and then encouraging the recruits to conduct such terrorist attacks in their home countries if they are unable to travel to Syria.[83] In March 2015,

> "the user of Twitter account @AbuHu55ain_, believed to be used at the time by an ISIS member located in Syria, tweeted: 'Lone Wolfs

---

78 *Id.*

79 Martin Chulov et al., *Isis Faces Exodus of Foreign Fighters as its 'Caliphate' Crumbles*, THE GUARDIAN (Apr. 26, 2017), https://www.theguardian.com/world/2017/apr/26/isis-exodus-foreign-fighters-caliphate-crumbles.

80 *Id.*

81 *See* Celestine Bohlen, *Why Do Terrorists Target Democracies?*, N.Y. TIMES (Sept. 15, 2015), https://www.nytimes.com/2015/09/15/world/why-do-terrorists-target-democracies.html.

82 *See* Nicole Chavez et al., *New York Attack Suspect Charged With Federal Terrorism Offenses*, CNN (Nov. 2, 2017), https://www.cnn.com/2017/11/01/us/new-york-attack/index.html (discussing the case of Sayfullo Habibullaevic Saipov, who was radicalized over the internet and carried out an attack all while in the U.S.).

83 Complaint at 4, United States v. Saipov, No. 17-MAG-8177 (S.D.N.Y. 2017), http://cdn.cnn.com/cnn/2017/images/11/01/u.s..v..sayfullo.saipov.complaint.pdf [hereinafter Complaint].

> Rise Up'; 'If you can't make the hijrah [to Syria], don[']t sit at home and give up . . . ignite a bomb, stab a kaffir ["disbeliever"], or shoot a politician!'; '[I]f you came here [to Syria], you'd be on the frontline fighting, right? But you couldn't come here, so why not fight the kuffar over there?'; and '[I] always see in the media brothers getting caught making hijrah, brothers know that your hijrah is not over just because you got stopped.'"[84]

Calls on social media such as these have led to over a dozen attacks both in the U.S. and Europe.[85] One such attack occurred on October 31st, 2017, when 29-year-old Sayfullo Habibullaevic Saipov from New Jersey drove a truck through a well-trafficked bike path in New York City where he killed eight people.[86] After the attack, the FBI found approximately 90 videos and 4,000 photographs consisting mainly of ISIS propaganda on Saipov's cell phone,[87] which Saipov confessed were his sources of inspiration for the attack.[88] According to officials, Saipov "appears to have followed almost exactly to a 'T' the instructions that ISIS has put out in its social media channels . . . on how to carry out such an attack."[89] These instructions were posted online in ISIS' official magazine called *Rumiyah* (formerly known as *Dabiq*) which encouraged vehicle attacks, followed by a gun and knife attack to "maximize the 'kill count' and terror."[90]

Similarly, in December 2017, 27-year-old Akayed Ullah attempted to detonate a bomb in a New York City subway station near Times Square.[91] After being taken into custody, Ullah confessed he had been radicalized over the internet and conducted the attack in response to the U.S. airstrikes in Syria and other regions of the caliphate.[92] Both Akayed and Saipov were charged with, among other things, knowingly providing material support

---

84 *Id.*

85 *See* Chavez et al., *supra* note 82 ("Since 2014, there have been 15 vehicular attacks in the West by jihadist terrorists. . . .").

86 *Id.*

87 *Id.*; Complaint, *supra* note 83, at 9.

88 Complaint, *supra* note 83, at 8.

89 Chavez et al., *supra* note 82.

90 Complaint, *supra* note 83, at 7.

91 Amanda Holpuch et al., *Manhattan Subway Explosion 'Was Attempted Terrorist Attack,' Says Mayor*, THE GUARDIAN (Dec. 11, 2017), https://www.theguardian.com/us-news/2017/dec/11/new-york-police-explosion-reports-manhattan.

92 *Id.*

to a known terrorist group, ISIS.[93]

C. Democratic Vulnerabilities Through Social Media: The First Amendment

In response to Ullah's attempted attack, New York Governor, Andrew Cuomo, stated, "[t]he reality is that we are a target by many who would like to make a statement against democracy, against freedom."[94] After 9/11, former U.S. President George W. Bush similarly explained that "America was targeted for attack because we're the brightest beacon for freedom and opportunity in the world."[95] With these freedoms however, comes vulnerabilities.[96]

While the U.S. generally celebrates its broad freedom of speech principles, the lack of restrictions against this freedom has allowed groups such as ISIS to spread its dangerous ideologies via social media sites.[97] This has led to a tough balancing act, whereby the U.S. government must weigh the national security interest of preventing terrorist attacks against its citizens' First Amendment free speech rights.[98]

Similar issues have formed in many European countries, whose citizens also enjoy freedom of speech rights.[99] The differences, however, can be seen when reviewing each country's legislative and judicial response to the issues. Countries "such as France and Germany have passed legislation that blocks pro-terrorist websites and holds information service providers ('ISPs') subject to prosecution if they provide access to hate speech sites."[100]

In contrast, the U.S. legislature has shied away from bills that not only would hold social media companies responsible for the dissemination of terroristic information, but those that would require social media companies to simply cooperate with the government by reporting terroristic propaganda found on its

---

93 Chavez et al., *supra* note 82; *id.*

94 Holpuch et al., *supra* note 91.

95 Bohlen, *supra* note 81.

96 *See id.*

97 *See* Jaclyn K. Haughom, *Combatting Terrorism in a Digital Age: First Amendment Implications*, FREEDOM F. INST. (Nov. 16, 2016), https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/.

98 *Id.*

99 *See id.*

100 *Id.*

sites.[101] This is due to the political nature of ISIS propaganda and the broad protection afforded political speech in the United States.[102] While speech that creates a "clear and present danger" is not protected under the U.S. Constitution,[103] restrictions on political speech are subject to the strictest of scrutiny – meaning that the government must have a compelling governmental interest in restricting the speech and employ the least restrictive means possible for prohibiting said speech.[104] This Constitutional principle is essential to a democratic and free society "to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[105] Furthermore, in *Texas v. Johnson*, 491 U.S. 397, 414 (1989), Justice Brennan made it clear that this protection was afforded to *all* political speech when he stated, "[i]f there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[106]

D. ISP Protections and Case Law

While an argument may be made that ISIS threats on social media, such as those from @AbuHu55ain_'s Twitter page quoted above, may constitute a clear and present danger as he seeks to incite violence and imminent harm through his followers' actions, liability claims brought against social media companies for allowing terroristic information to be posted have generally failed.

i. Anti-Terrorism Act Section 2339A and 2339B: The Material Support Statute

Section 2339A of the Anti-Terrorism Act ("ATA") states that:

---

101 *Id.*

102 *See* Eric Posner, *ISIS Gives Us No Choice but to Consider Limits on Speech*, SLATE (Dec. 15, 2015), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.html.

103 Schenck v. United States, 249 U.S. 47, 52 (1919).

104 *See generally* Texas v. Johnson, 491 U.S. 397, 412 (1989) (quoting Boos v. Barry, 485 U.S. 312, 318 (1988)) (concluding that the restriction on political speech is subject to "the most exacting scrutiny").

105 New York Times Co. v. Sullivan, 376 U.S. 254, 269 (1964) (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).

106 *Johnson*, 491 U.S. at 414.

> Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or carrying out, a violation of [various terrorist activity statutes] or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.[107]

Relatedly, section 2339B provides that:

> Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years. . . . To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization . . . or that the organization has engaged or engages in terrorism. . . .[108]

The purpose of section 2339A is to prohibit people from providing material support to the commission of terroristic offenses, while section 2339B prohibits providing material support to known terrorist organizations themselves.[109]

In *Fields v. Twitter, Inc.*, 881 F.3d 739 (9th Cir. 2018), the plaintiffs sued Twitter, claiming that the company violated section 2339A and section 2339B of the ATA when it provided material support to ISIS by allowing known terrorists to establish Twitter accounts and use them to post pro-terroristic materials.[110] Specifically, they argued that Twitter's failure to shut-down the "estimated 70,000 Twitter accounts, at least 79 of which were 'official,'"[111] was the proximate cause of their husbands' deaths because it allowed ISIS members to communicate, organize, and encourage the terrorist attack that killed their husbands.[112] The Ninth Circuit, however, rejected this argument and dismissed the case, finding that for purposes of the ATA, a "direct relationship,"

---

107 18 U.S.C. § 2339A(a) (2012).

108 18 U.S.C. § 2339B(a)(1) (2012).

109 CHARLES DOYLE, CONG. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C § 2339A AND § 2339B 1 (2016).

110 Fields v. Twitter, Inc., 881 F.3d 739, 742-43 (9th Cir. 2018).

111 *Id.* at 742.

112 *Id.*

rather than the proximate cause foreseeability standard, was required to hold Twitter liable for these deaths.[113]

Similarly, in *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150 (N.D. Cal. 2017), the plaintiffs alleged that Google provided material support to ISIS when the company allowed ISIS members, (specifically, two of the twelve terrorists who conducted an attack in Paris in 2015 that killed their son), to upload and share "jihadi" YouTube videos when Google had the ability to shut-down such accounts and videos.[114] ISIS also used YouTube to claim responsibility for the 2015 attack on Paris.[115] Furthermore, Plaintiffs condemned Google for allowing ISIS to advertise itself on YouTube and allowing the advertisements to be broadly circulated due to the company's advertisement algorithms.[116] Notwithstanding these arguments, the Northern District of California Court granted Google's motion to dismiss by relying on the often-litigated section 230 of the Communications Decency Act.[117]

ii. Communications Decency Act Section 230(c)(1)

Section 230(c)(1) of the 1996 Communications Decency Act ("CDA") protects information service providers ("ISPs") by stating, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[118] This provision shields companies such as Facebook, Twitter, and Google from being both civilly and criminally liable for allowing terroristic information to be posted by other users, or failing to remove such content once it is posted.[119]

Just as in the cases against Twitter and Google discussed above, the plaintiffs in *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140 (E.D.N.Y. 2017) sued Facebook for allegedly "recruiting, gathering information, planning, inciting, [ ] giving instructions for terror attacks, . . . issu[ing] terroristic threats, . . . [and] intimidating and

---

113 I*d.* at 748.
114 Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150, 1154–55 (N.D. Cal. 2017).
115 *Id.* at 1154.
116 *Id.* at 1155.
117 *Id.* at 1170–71.
118 47 U.S.C. § 230(c)(1) (2012).
119 *See* Haughom, *supra* note 97; Cohen v. Facebook, Inc., 252 F. Supp. 3d 140, 157 (E.D.N.Y. 2017).

coerc[ing] civilian populations."[120] The plaintiffs alleged that Palestinian terrorist organizations used Facebook to disseminate incitements to violence – "including commands to murder Israelis and Jews" – while Facebook's owners did little to prevent such incitement or deactivate such terroristic accounts.[121] Following the trend of cases against Twitter and Google, the Eastern District of New York Court found that Facebook was immune from liability under CDA section 230(c)(1) and granted Facebook's motion to dismiss the case for failure to state a claim.[122] In doing so, the court affirmed prior court decisions, holding "that decisions as to the 'structure and operation' of a website [and] decisions as to who may obtain a [social media] account" also fall within section 230(c)(1)'s protection.[123]

E. Proposed Legislation

In addition to the Material Support Statute and section 230(c)(1) of the CDA, the U.S. legislature introduced H.R. 3654, Combat Terrorist Use of Social Media Act of 2015, which would require the President to submit a report to Congress outlining U.S. strategy for combating terrorism on social media.[124] The bill was passed by the House but rejected by the Senate and therefore, not enacted as law.[125] A second attempt to enact the bill came in February 2016, when S. 2517, Combat Terrorist Use of Social Media Act of 2016 was introduced.[126] A report by the Committee on Homeland Security and Governmental Affairs was issued in July 2016, but no further action was taken on the bill.[127] Another attempt was made in early 2016 when H.R. 4820, the Combatting Terrorist Recruitment Act of 2016 was introduced,[128] which would "require

---

120 *Cohen*, 252 F. Supp. 3d at 157.

121 *Id.* at 147.

122 *Id.* at 158, 161.

123 *Id.* at 157.

124 Combat Terrorist Use of Social Media Act of 2015, H.R. 3654, 114th Cong. (2015).

125 *H.R. 3654 (114th): Combat Terrorist Use of Social Media Act of 2015*, GOVTRACK https://www.govtrack.us/congress/bills/114/hr3654 (last visited Dec. 4, 2018).

126 *See* Combat Terrorist Use of Social Media Act of 2016, S. 2517, 114th Cong. (2016).

127 *S. 2517 (114th): Combat Terrorist Use of Social Media Act of 2016*, GOVTRACK https://www.govtrack.us/congress/bills/114/s2517 (last visited Dec. 4, 2018).

128 *See* Press Release, Congressman Chuck Fleischmann, Fleischmann's Bill to Combat Terrorism Passes House, (Apr. 27, 2016),

the Secretary of Homeland Security to use the testimonials of former violent extremists or their associates in order to counter terrorist recruitment. . . . "[129] This bill too, however, was never enacted as it was only passed by the House.[130]

F. "Best Practices" Guidelines and Self-Regulation of Social Media Sites

Since past legislative attempts have largely failed in recent years, some Americans are looking to federal agencies to create "best practices" guidelines for combating terrorism on social media.[131] Just as the Federal Trade Commission created "best practices" guidelines for businesses with regards to protecting consumer privacy, it has been suggested that the Department of Homeland Security develop "best practices" for social media companies to help them prevent, detect, and deter pro-terroristic activities on their websites.[132] While social media sites would not be bound by such guidelines, such methods of self-regulation would deem governmental interference unnecessary, which in turn would prevent the U.S. government from infringing upon its citizens' First Amendment free speech rights.[133]

In the realm of self-regulation, Twitter announced it had suspended approximately 360,000 ISIS-linked accounts found to be "threatening or promoting terrorist acts" from mid-2015 to August 2016.[134] Some, however, still found these actions unsatisfactory as ISIS accounts were easily re-established after being suspended.[135] Further, while the company does not allow its

---

https://fleischmann.house.gov/media/press-releases/release-fleischmanns-bill-combat-terrorism-passes-house.

129 Combating Terrorist Recruitment Act of 2016, H.R. 4820, 114th Cong. (2016).

130 *See H.R. 4820 – Combating Terrorist Recruitment Act of 2016*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/4820/actions (last visited Dec. 4, 2018).

131 Haughom, *supra* note 97.

132 *Id.*

133 *See id.*

134 Anne Cameron Cain & Beatriz Gonzalez, *Twitter Must Do More to Block ISIS*, N.Y. TIMES (Jan. 13, 2017), https://www.nytimes.com/2017/01/13/opinion/twitter-must-do-more-to-block-isis.html; s*ee also* Nicky Woolf, *Twitter Suspends 235,000 Accounts in Six Months For Promoting Terrorism*, THE GUARDIAN (Aug. 18, 2016), https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis.

135 *See* Cain & Gonzalez, *supra* note 134; *see also* Rick Gladstone, *Twitter Says*

users to make threats or promote violence and terrorism, it stated that "Twitter continues to strongly support freedom of expression and diverse perspectives. . . . "[136] Facebook on the other hand, whose spokesman claimed that the company works aggressively to identify and remove ISIS-related material, was deemed "the leader and the best at removing [terroristic] content" by the executive director of Middle East Media Research, Steve Stalinsky.[137]

To further encourage self-regulation, the U.S. Senate Committee on Commerce, Science, and Transportation held a hearing in January 2018 at which Facebook, Twitter, and Google publicly testified to their self-regulation efforts and progress in fighting terrorism on their websites.[138] Facebook's spokesperson testified that the company "is now able to remove 99 percent of ISIS and Al-Qaeda-related posts before reaching a human flagger. . . . " which she attributes to Facebook's AI platform.[139] The spokesperson claims this AI machine-learning technology is being used to identify pro-terrorist material, prevent ISIS-related content from being re-uploaded, and preventing users from creating a new profiles after their profile has been suspended.[140] Similarly, Google's YouTube expressed that its machine-learning program is able to remove 98 percent of the terroristic content found on its site, with "70 percent [being] removed within eight hours."[141] Likewise, Twitter claims to have suspended over one million accounts linked to terrorism since 2015 with the help of new technology platforms.[142] Additionally, Facebook hired over 3,000 people who will join the review team and work "to identify all content that violates the community standards, including extremist content," while YouTube announced it will not be providing monetary compensation to videos that fall into the "gray area" – videos containing questionable content but that do not qualify as being a violation of company policy.[143]

---

it Suspended 10,000 ISIS-Linked Accounts in One Day, N.Y. TIMES (Apr. 9, 2015), https://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html.

136 Julia Greenberg, *Why Facebook and Twitter Can't Just Wipe Out ISIS Online*, WIRED (Nov. 21, 2015), https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/.

137 *Id.*

138 *See* Grigonis, *supra* note 44.

139 *Id.*

140 *Id.*

141 *Id.*

142 *Id.*

143 *Id.*

G. Conclusion

As the fear of ISIS recruitment on social media sites and lone wolf attacks remain a threat to both American safety and democracy, the need for security is obvious. The U.S. legislature has repeatedly struck down bills aimed at forming a plan to combat terrorism on social media. The U.S. judiciary has consistently rejected the idea of holding social media sites responsible for both terrorist propaganda posted on the websites and the effects of such propaganda on U.S. citizens. With governmental inaction such as this, pressure has been placed on social media companies to self-regulate the content posted on its site despite deeply-rooted freedom of speech principles. Past attempts to self-regulate have been challenged as many believe the companies have not done enough to eradicate terrorist information from their sites.[144] This time, however, major sites such as Facebook, Twitter, and Google have announced seemingly effective machine-learning technology designed to prevent and shut-down terrorist information on the companies' sites, and prevent the resurrection of such profiles[145] – which were some of the complained-of inefficiencies in the companies' past attempts.[146] Since the use of such technology is still in its early stages, however, it will take some time to determine whether this most recent attempt to self-regulate is sufficient, or whether further attempts at creating legislation is needed.

IV. CONCLUSION

While legislation requiring social media sites to monitor foreign political ads has been met with less resistance than that requiring social media sites to monitor ISIS propaganda, self-regulation of such sites has been considered a viable option for combating both threats to U.S. democracy. But can we rely on self-regulation alone to solve such intrusive threats? Do we even have other viable options when political differences and the U.S. Constitution prevent the legislature and judiciary from creating obligations for social media sites to follow?

---

144 Leandra Bernstein, *Are Social Media Companies Doing Enough to Stop DIY Terrorism?*, WJLA (Nov. 1, 2017), http://wjla.com/news/nation-world/are-social-media-companies-doing-enough-to-stop-terrorism.

145 *See* Grigonis, *supra* note 44.

146 *See* Cain & Gonzalez, *supra* note 134.

Because democracy is a system of government in which the *State's citizens* are to vote for their political leaders, the U.S. government has deemed it compelling and necessary to eliminate foreign influence in our election by prohibiting "foreign nationals" from making any contributions or donations to U.S. elections, including through advertisements.[147] Allowing social media companies to claim a "small items" exception is no longer appropriate given the magnitude of foreign influence found on social media sites during the 2016 U.S. Presidential Election.[148] Despite expressing disapproval of the Honest Ads Act, Facebook, Google, and Twitter have all expressed intentions to self-regulate their sites by requiring disclosure of the ad-owner's identity, presumably preventing foreign nationals from creating U.S. election materials and allowing users to see whose money and influence is behind every ad.[149]

With the broad protections afforded to political free speech in the U.S., the government's ability to eradicate ISIS propaganda from social media sites is limited.[150] Thus, the trend of self-regulation continues as social media companies are left with the pressure of placing its own regulations on its sites' content.[151] This trend comes though, only after multiple attempts by the U.S. legislature to enact regulatory laws and numerous court cases in which families of those killed by terrorist organizations attempt to hold social media companies liable for their family members' deaths.[152] But while past attempts at self-regulation were arguably insufficient, the promise of new machine-learning technology and the expansion of social media review teams may just be the strict measures necessary to prevent ISIS from influencing and recruiting American citizens via social media. Because the Honest Ads Act and self-regulatory methods are still in their infancy, results and public opinion regarding the regulations during the next year will be a good indication of whether self-regulation is effective in protecting U.S. democracy, or whether alternative measures must be found.

---

147 Martin, *supra* note 31.

148 *See* Shaban et al., *supra* note 4 (explaining the introduction of the Honest Ads Act).

149 *See* Isaac & Shane, *supra* note 26; Shaban et al., *supra* note 4; Grigonis, *supra* note 45.

150 *See generally* Texas v. Johnson, 491 U.S. 397 (1989) (explaining the restrictions on the government's ability to restrict unfavored speech).

151 *See* Grigonis, *supra* note 44.

152 *See supra* Part III sections (D) and (E) (discussing the issue at length).