CLC

ADVANCING DEMOCRACY THROUGH LAW

15 YEARS

Examining Foreign Interference in U.S. Elections

A report from the Campaign Legal Center

With articles authored by:

Trevor Potter, Campaign Legal Center

Brendan Fischer, Campaign Legal Center

Douglas Guilbeault, University of Pennsylvania's Annenberg School for Communication, with Robert Gorwa, Department of Politics and International Relations at the University of Oxford

Daniel A. Petalas, Garvey Schubert Barer

Max Bergmann, Center for American Progress

January 2018

CLC

ADVANCING
DEMOCRACY
THROUGH LAW

15 YEARS

In October 2017, Campaign Legal Center (CLC), with support from the Democracy Fund, held a full-day event in Washington, D.C., convening legal experts, academics, journalists, and practitioners from across disciplines to address the pressing matter of foreign interference in U.S. elections. This report captures the breadth of the issues discussed at the convening, considers the challenges to and opportunities for protecting the integrity of our elections, and concludes with recommendations for action so that U.S. elections are decided by U.S. citizens.

ACKNOWLEDGMENTS

The Campaign Legal Center thanks the Democracy Fund for the generous support that made the conference and this report possible.

We would like to thank the following panelists and moderators for participating in the conference that inspired this report: Dana Priest, Michael Isikoff, Sandhya Bathija, Adav Noti, Joseph Lorenzo Hall, Daniel Petalas, Tara Malloy, Max Bergmann, Andrew C. Kuchins, Laura Rosenberger, Norm Ornstein, David Kolker, Pippa Scarlett, Douglas R. Guilbeault, and Larry Noble.

We are also grateful to all of the report's contributors, to Maan Sacdalan, who designed the final product, and to Maggie Christ and other Campaign Legal Center staff who provided input.

EXECUTIVE SUMMARY

Beginning with a bitter war of independence from England, followed by active interference in U.S. politics by representatives of the French revolutionary government in the late 1700s, through Nazi support of the German-American Bund in the 1930s, to concerns that millions in Chinese funds flowed to the Democratic Party in the 1990s, trepidation about foreign influence over our democracy is as old as the United States itself.

Either as a young and vulnerable republic or as a world power, the U.S. has seen repeated attempts by foreign powers to affect its politics and policies.

In 2016, of course, the most obvious foreign influence came from Russia. The intelligence community is in agreement on that. But while we continue to learn something new every day about the *particular* ways Russia attempted to undermine our democracy, other countries are taking note. In 2018, it could be North Korea, China, Iran, or any number of other foreign countries or actors with an interest in influencing or disrupting U.S. democracy.

Disputes over whether foreign meddling in 2016 affected election results are not productive. Rather, we must devote national resources to addressing the host of vulnerabilities that the 2016 election exposed:

- Secret foreign spending on digital political ads demonstrated how campaign finance laws and disclosure requirements have failed to catch up to the digital age;
- Foreign-controlled money funneled to at least one U.S. super PAC and other schemes to secretly route foreign funds into U.S. elections revealed how *Citizens United* created new avenues for foreign influence;
- The dissemination of social media messages through automated "bots" exposed vexing new challenges for policymakers, online platforms, and the public;
- Attempted hacking into states' voting systems revealed potential flaws in our election security regime; and
- Our inability to deter foreign actors from trying any of the above showed the limits of our foreign policy.

Left unaddressed, these vulnerabilities will only be exploited to greater effect by other foreign actors in 2018 and beyond. This report's goal is to explore solutions that will prevent such exploitation—not to mention protect the foundations of our democracy—and to that end, makes the following recommendations:

The Federal Election Commission (FEC) and internet platforms should require political advertisers to identify themselves to voters. Requiring disclaimers stating who paid for digital political ads should be an easy fix. Both the FEC and some internet platforms are already making progress in this direction, but more must be done.

Congress should strengthen disclosure laws, including by passing the bipartisan HONEST Ads Act. The bipartisan HONEST Ads Act would shore up other digital gaps in campaign finance law exploited by Russia in 2016. The Act would do so by requiring disclaimers and disclosure for digital ads mentioning a candidate shortly before an election—just as television and newspaper ads currently do—and creating greater transparency around the content of the ads themselves. Congress should also enact disclosure legislation to close the transparency loopholes that still allow foreign governments and individuals to secretly launder money into U.S. elections. And Congress should hold hearings and gather information to determine whether and how foreign money spent on genuine issue advocacy should be treated differently than foreign money spent on electioneering.

Further research and analysis are needed to develop an effective approach to social media bot activity. The emerging trend of fake social media accounts and automated bots to disseminate political messages presents vexing challenges for policymakers and social media companies alike. There must be a careful assessment as to which elements of bot policy should be within the control of government and which should be left to self-regulation. More research is certainly needed on how political actors spend money to disseminate messages through bots or other forms of automation.

The public and private sectors should strengthen voters' media literacy. Even if new online transparency policies are implemented—and especially if they are not—civic society has an important role to play in improving voters' media literacy in the midst of an increasingly complex online landscape.

Congress must bolster our election infrastructure security and modernize voting equipment. Any effort to guard against future foreign meddling requires protecting our election infrastructure. This includes bolstering security resources available to the states and providing funds for modernizing voting equipment, preparing election officials for the newest threats, and continually testing and improving election systems across the country.

Addressing foreign interference must be treated as a national priority. The U.S. must treat foreign meddling in our elections as an urgent national security threat, and take decisive action to deter and defend against efforts to intervene in American democracy.

The unfortunate reality is that discussion of Russian activities in the 2016 election has become mired in partisan politics. Yet we must look past the 2016 history to provide security for future elections.

Our country's long-standing concerns about foreign interference are rooted in basic notions of democratic self-governance and national sovereignty. Addressing these concerns is about protecting the foundations of our democracy.

Fortunately, while the problems may seem daunting, many of the solutions are relatively simple. But the responsibility of protecting our democracy from these threats does not lie with any single entity. Congress must react to these threats and also be *proactive* in anticipating future vulnerabilities. The FEC must do its job in enforcing the law, which includes responding to new challenges presented by the digital age. Internet companies must fully come to terms with the power of their platforms and work with government to protect against those seeking to do our democracy harm. And we all must ensure that voters have the tools to critically evaluate digital information.

Unless all of these actors begin to work toward solutions, there is every reason to believe that the actual or attempted foreign meddling of 2016 will become a much greater threat in elections to come.

TABLE OF CONTENTS

ABOUT THE CONFERENCE

In October 2017, Campaign Legal Center (CLC), with support from the Democracy Fund, held a full-day event in Washington, D.C., convening legal experts, academics, journalists, and practitioners from across disciplines to address the pressing matter of foreign interference in U.S. elections. (A full video of the conference is available at http://bit.ly/foreigninterference.)

Although the matter became politically charged in 2017, foreign meddling in elections poses a unique threat to democratic self-governance and national sovereignty. CLC therefore designed the convening to set aside partisan rhetoric and instead to engage in a grounded, expert analysis of the current state of the law and its shortcomings.

The conference kicked off with presentations from *The Washington Post*'s Dana Priest and *Yahoo News'* Michael Isikoff, who laid the factual groundwork for what we know happened in the 2016 election: the attempted interference with our elections through such activities as the hacking of emails and databases, the dissemination of political messages through paid and unpaid social media, and the government's confused and confusing response. Both offered important context. Priest provided an international perspective, describing how some former Soviet bloc countries have become accustomed to Russian meddling—but that elected officials, citizens, journalists, and law enforcement in those countries have developed the tools to counter that influence. Isikoff noted that in the 2008 U.S. elections, China launched a massive cyberespionage operation against both major parties' presidential campaigns—but that the U.S. nonetheless failed to halt a more successful hacking effort in 2016.

Next, Daniel Petalas, former acting general counsel and head of enforcement at the Federal Election Commission (FEC) and a federal corruption prosecutor at the Department of Justice's (DOJ's) Public Integrity Section, described the tools that federal prosecutors have to address foreign meddling as well as the challenges in putting together a successful case. Petalas authored the article in this report, *Foreign Interference in Federal Elections: Criminal Tools and Vulnerabilities*.

CLC's Adav Noti, a former associate general counsel for policy at the FEC, described how, despite the apparent breadth of federal campaign finance law's ban on foreign nationals spending money in U.S. elections, the law's effectiveness is limited by 21st century campaign practices. Joseph Lorenzo Hall from the Center for Democracy & Technology (CD&T) outlined some of the technological vulnerabilities in U.S. election infrastructure; he emphasized that in at least two instances, foreign actors managed to compromise state election support systems, and multiple other states were targeted as well. Fortunately, Hall noted, there are a number of simple fixes that could be implemented to improve election cybersecurity, but federal laws like the Digital Millennium Copyright Act (DMCA) can be a barrier for groups like CD&T in assessing election infrastructure vulnerabilities and identifying solutions.

U.S. domestic laws are only one element of efforts to protect the sovereignty of our democracy and limit foreign interference. Max Bergmann, a former State Department official and current fellow at the Center for American Progress, emphasized how strategic signaling in U.S. foreign policy plays a critical role in deterring election meddling on the international stage. Bergmann contributed the article *America's First Line of Defense May Have Failed in 2016*.

Dr. Andrew Kuchins of the Center for Eurasian, Russian and East European Studies (CERES) at Georgetown University provided insight into Russia's motivations for its 2016 interference efforts and emphasized that Russia will try again, more carefully, in future elections. Next, Laura Rosenberger, of the Alliance for Securing Democracy and a senior fellow at the German Marshall Fund, emphasized the importance of coordinating with international partners to counter meddling by actors like Russia, and the important role of the business community and civil society in shoring up vulnerabilities.

Douglas Guilbeault, a researcher in the Network Dynamics Group and a Ph.D. candidate at the Annenberg School, discussed how the rise of automated online activity presents new challenges for regulators and social media companies alike—but he argued that policymakers should proceed cautiously in this highly complex area. Guilbeault contributed the article *Current Challenges for Bot Policy and Foreign Interference* (co-authored with Robert Gorwa).

Philippa Scarlett, a former White House deputy intellectual property enforcement coordinator, discussed models for how government can convene the business community to develop solutions. And CLC's David Kolker, a former head of litigation at the FEC, discussed the options for Congress, the FEC, and state and local governments to develop new legislation and regulations to shore up some of the campaign finance vulnerabilities exposed in the 2016 elections.

This report captures the breadth of the issues discussed at the convening, considers the challenges to and opportunities for protecting the integrity of our elections, and concludes with recommendations for action so that U.S. elections are decided by U.S. citizens.

CLC's President Trevor Potter, a former DOJ official and FEC chair, opened the conference by placing the convening's theme in historical context. As he outlines, at multiple points in our history, the United States has been concerned about foreign agents meddling in our democracy. This article is an expanded version of his remarks.

Foreign Interference in the 2016 Election: How Did We Get Here?

By Trevor Potter

Trevor Potter is the founder and president of the Campaign Legal Center and a former Republican chairman of the Federal Election Commission.

While they may not have envisioned the digital age, the Founding Fathers certainly worried about the possibility of foreign interference in our elections—the possibility that foreign powers would wish our democracy ill and attempt to frustrate its election process, or influence the results in ways that would benefit their own interests.

An early moment of concern came in 1785, when Louis XVI presented Benjamin Franklin with a snuff box that displayed a diamond-framed portrait of the French king.[1] As Zephyr Teachout has documented, the opulent gift caused considerable anxiety in the United States about the French monarch buying influence and loyalty from American officials, especially as many were already suspicious of Franklin's close relationship with France.[2]

Although Congress eventually allowed Franklin to keep the gift, the incident foreshadowed a concern about foreign influence that would endure for centuries.

When actually drafting the Constitution, the Framers continued to worry about the influence of foreign actors. In the *Federalist Papers*, Alexander Hamilton explicitly expressed concern about "desire in foreign powers to gain an improper ascendant in our councils."[3] Concerns like these lurked beneath the surface of many of the Framers' decisions. For example, the Framers initially considered allowing treaties to pass with a simple majority of senators' votes, but, after Elbridge Gerry warned that this could facilitate foreign corruption, they settled on a two-thirds majority.[4] As additional signs of their concerns, the Framers also included guardrails like the requirement that the president be a "natural born citizen" rather than a foreign-born aristocrat, and the Emoluments Clause, which prohibits federal officials from taking any "emolument"—any gift or service—from foreign governments.

Alexander Hamilton warned of the "desire in foreign powers to gain an improper ascendant in our councils."

However, despite these constitutional safeguards, concerns about foreign influence soon arose again. In 1793, Edmond Charles Genêt, the U.S. representative from France, by then a revolutionary government, sought an alliance with the U.S. against Britain but was rebuffed by the U.S. government, which had adopted a strict policy of neutrality. Genêt then sought to bypass official government opposition and appealed to the American public, enraging Washington, who was struck by Genêt's "defiance" of the U.S. government and his recklessness in "threaten[ing] the Executive with an appeal to the People."[5]

French meddling arose again during the 1796 election. Earlier in the year, Washington had given his Farewell Address, in which he warned explicitly about the "insidious wiles of foreign influence":

> Against the insidious wiles of foreign influence (I conjure you to believe me, fellow-citizens) the jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republican government.[6]

In the same speech, Washington warned that foreign forces could exploit American political divisions: "the spirit of party … opens the door to foreign influence and corruption, which finds a facilitated access to the government itself through the channels of party passions. Thus the policy and the will of one country are subjected to the policy and will of another."[7]

That year's election to choose Washington's replacement would include one potentially "insidious wil[e] of foreign influence" in the form of French meddling. France was angered by the signing of the 1795 Jay Treaty between Britain and the United States, and saw the upcoming presidential election as an opportunity to regain favor in American foreign policy. So, just before the election, French ambassador Pierre Auguste Adet published pieces in a Philadelphia newspaper "warning," as Professor Stuart Leibiger characterized them, "that unless the pro-French Republican candidate Thomas Jefferson defeated pro-British Federalist John Adams in the presidential election, the result would be war between the United States and France."[8]

Although France's preferred candidate did not ultimately prevail in the election, Adet's antics continued to trouble Framers like James Madison. In a letter to his father just after the election, Madison referred to the "Remonstrance of Mr. Adet against our Govt," and expressed concern that "the consequences must prove very serious in various respects" if the French-American relationship were not repaired.[9]

These concerns have continued to arise throughout U.S. history.

In the early years of the 20th century, for example, the U.S. faced another type of foreign threat at home. In 1936, the German American Bund was established with ties to the Nazi government in Germany. It distributed propaganda, organized youth camps, and held rallies, including a large rally at Madison Square Garden in February 1939 in which the assembled members denounced President Roosevelt and cried "Heil Hitler."[10]

In response to concerns about the influence of German-supported groups like these, Congress passed the Foreign Agents Registration Act, or FARA, in 1938.[11] With the exception of certain exempted parties, FARA mandates that "every person who becomes an agent of a foreign principal shall, within ten days thereafter, file with the Attorney General, in duplicate, a registration statement, under oath on a form prescribed by the Attorney General."[12] Foreign agents also must report any "informational materials" they intend to distribute in the United States.[13]

In the 1990s, it was potential Chinese influence over the Clinton administration and the Democratic Party that drew concern. The Senate Governmental Affairs Committee's report *Illegal or Improper Activities in Connection with 1996 Federal Election Campaigns* raised questions about $1.6 million in contributions organized by two Democratic Party fundraisers, John Huang and Ted Sioeng.[14] The Committee found that of the $400,000 that Sioeng gave to the Democrats, at least half came from foreign sources.[15] After the election, the Democratic National Committee returned almost $3 million in various suspect contributions, including funds raised by Huang.[16] Later, in 2002, the FEC levied a record-breaking $719,000 in fines against the DNC, the Bill Clinton campaign, and various individuals and corporations for soliciting illegal foreign contributions in 1996.[17]

Partially in response to those scandals, Congress in 2002 enacted the Bipartisan Campaign Reform Act (BCRA), which, among other things, strengthened the foreign national prohibition and banned unregulated "soft money" that masked foreign spending.

In the years since, the Department of Justice has prosecuted several foreign national cases. In 2014, for example, federal prosecutors brought a case against a Mexican tycoon who they alleged "funneled more than $500,000 into U.S. political races through super PACs and various shell companies" in support of three Democratic politicians and San Diego's Republican district attorney.[18]

In 2016, of course, the most obvious foreign influence came from Russia—and the interference may have been broader and more multifaceted than anything the U.S. had experienced before. We've faced the remarkable sight of U.S. intelligence agencies collectively testifying before Congress of their certainty that the Russian government attempted to interfere in multiple parts of the electoral process. And we have seen the indictment of a sitting president's past campaign manager and his National Security Advisor as part of an ongoing investigation into foreign meddling. From the targeted theft of emails from political parties to purported offers of opposition research, from secret social media advertising campaigns to attempted hacking of state election systems, Russia's efforts exposed serious vulnerabilities in U.S. laws and practices.

The full extent of foreign influence in the 2016 election is not yet known. And the importance of this issue goes far beyond the 2016 election. It is about protecting the foundations of our democracy, particularly in a world that is increasingly moving online. What the 2016 election did do was expose a host of vulnerabilities.

How did we get here? One way is that the years since the Supreme Court's *Citizens United* decision have seen the growth of undisclosed money flowing into our elections. This is directly contrary to the stated justifications of Justice Anthony Kennedy in the *Citizens United* opinion, where he wrote that "transparency enables the electorate to make informed decisions and give proper weight to different speakers and messages."[19] When groups that don't disclose their donors spend hundreds of millions influencing elections, voters can't see where political spending is truly coming from. This provides an attractive opening for foreign interests to influence our elections without any scrutiny by voters, the press, or regulatory entities.

At the same time, as political campaigning increasingly moves online, Congress and the Federal Election Commission have failed to update our campaign finance laws for the digital age. In the 2016 elections, $1.4 *billion* was spent on digital political ads, but U.S. voters were often left in the dark about who was paying for those online ads.[20] It was only after the election that we learned the Russian government was behind thousands of Facebook political ads that reached at least 10 million Americans, and that much of this online activity was targeted to only a few key "swing" states.[21] A bipartisan group of senators has introduced legislation to close some of these online transparency loopholes, but the HONEST Ads Act has yet to receive a hearing.

One of the realities underlying these questions of the nature and extent of foreign interference is that such questions are often perceived to have partisan overtones because the most recent examples involved the 2016 presidential election.

But history proves that these are matters that should be of concern to all Americans, regardless of party, who care about the future of our democracy. A party or candidate who receives illegal foreign "help" today could well be on the other end of foreign spending tomorrow.

And the U.S. is not alone in these matters.

In Britain, academics have revealed that thousands of Russian Twitter accounts tweeted about Brexit during that campaign, including at least 419 operated by the Russian Internet Research Agency.[22] While Theresa May so far has resisted explicitly accusing Russia of meddling in Britain's 2016 vote to leave the European Union, she has—in broader terms—harshly criticized Russia's efforts to "undermine free societies," and has supported Parliament's Intelligence and Security committee investigating possible interference in Britain.[23] Other countries have been even more proactive. In response to concerns of interference in the French presidential elections, the French government introduced a cybersecurity seminar for French political parties, newspapers took steps to help voters identify false or misleading news reports, and the president called for a "mobilization of all the means necessary" against Russian cyberattacks.[24]

Germany also instituted a number of safeguards to protect against Russian interference in its 2017 elections.[25] For example, all votes are cast on hand-counted paper ballots, the German Federal Office for Information Security conducted rigorous pre-election testing of the election authority's computer systems, the Federal Security Council is developing a "hack-back" plan to proactively disarm foreign hackers, and German government officials continually warn of cyber threats from foreign actors seeking to undermine German elections.[26] Observers have also noted that trust in traditional news sources remains high in Germany—and that there is significant skepticism of news on social media.[27] These attitudes may help limit how effective foreign meddlers can be in sowing discord and in spreading false information on social media.

In Australia, the concerns about foreign interference revolve around China. In December 2017, a senator was forced to resign amid allegations that he was too influenced by his Chinese donors.[28] And 2017 was consumed by "damaging media reports about efforts by actors linked to the Chinese Communist Party to influence politics, media, and academia in Australia, as well as 'grave warnings' stemming from a classified Australian Security Intelligence Organisation report to the prime minister."[29] The Australian prime minister announced a package of reforms that would require foreign lobbyists to register, as FARA does in the United States, and would introduce new criminal penalties for violations related to foreign interference (including, potentially, donating to Australian political parties), among other changes.[30]

We cannot know which countries will seek to interfere with U.S. elections in the future. We could, for example, easily be looking at Chinese, Iranian, or North Korean activity in the coming years. All of those countries are known to have enormous cyber capacities and obvious interests in either affecting U.S. elections or disrupting them.

Because foreign interference is an attack on the integrity of our elections, it would be irresponsible to pretend that the efforts to undermine our elections will not continue.

This is not about one election. It is about all elections—it is about our democracy.

[1] Zephyr Teachout, Corruption in America 1-2 (2014).

[2] *Id.* at 25-6.

[3] The Federalist No. 68 (Alexander Hamilton).

[4] Teachout, *supra* note 1, at 80.

[5] *See* STANLEY ELKINS & ERIC MCKITRICK, THE AGE OF FEDERALISM 3511 (1993).

[6] *Washington's Farewell Address 1796*, Yale Avalon Project, http://avalon.law.yale.edu/18th_century/washing.asp (last visited Dec. 4, 2017).

[7] *Id.*

[8] Stuart Leibiger, *Historical meddling: The French connection*, Philadelphia Inquirer (Dec. 25, 2016), http://www.philly.com/philly/opinion/20161225_Historical_meddling__The_French_connection.html.

[9] *From James Madison to James Madison, Sr., 27 November 1796*, National Archives, http://founders.archives.gov/documents/Madison/01-16-02-0273 (last modified Nov. 26, 2017).

[10] German American Bund, U.S. Holocaust Memorial Museum, https://www.ushmm.org/wlc/en/article.php?ModuleId=10005684#/ (last visited Dec. 4, 2017).

[11] *FARA Frequently Asked Questions*, U.S. Department of Justice, https://www.fara.gov/fara-faq.html (last visited Dec. 4, 2017).

[12] 22 U.S.C. § 612(a).

[13] 22 U.S.C. § 614.

[14] U.S. Senate, Rept. 105-167, Investigation of Illegal or Improper Activities in Connection with 1996 Federal Election Campaigns: Final Report of the Committee on Governmental Affairs (1998).

[15] *Id.*

[16] Dan Balz, *Democrats Return $1.4 Million in Questionable Donations*, Wash. Post (June 28, 1997), http://www.washingtonpost.com/wp-srv/politics/special/campfin/stories/return.htm.

[17] Thomas B. Edsall & Edward Walsh, *FEC Issues Record Fines in Democrats' Scandals*, Wash. Post (Sept. 21, 2002), https://www.washingtonpost.com/archive/politics/2002/09/21/fec-issues-record-fines-in-democrats-scandals/2d2ed242-98e1-40a8-8574-caef4b7570e3/?utm_term=.41a641b03076.

[18] John Hudson, *Feds: Mexican Tycoon Exploited Super PACs to Influence U.S. Elections,* Foreign Policy (Feb. 11, 2014), http://foreignpolicy.com/2014/02/11/feds-mexican-tycoon-exploited-super-pacs-to-influence-u-s-elections/.

[19] *Citizens United v. FEC*, 558 U.S. 310, 371 (2010).

[20] Kip Cassino, *What Happened to Political Advertising in 2016 (and forever)*, Borrell Associates, Inc. (2017). *See also* Kate Kaye, *Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast Down 20%, Cable and Digital Way Up*, AdAge (Jan. 3, 2017), http://adage.com/article/media/2016-political-broadcast-tv-spend-20-cable-52/307346/.

[21] David Ingram, *Facebook says 10 million U.S. users saw Russia-linked ads*, Reuters (Oct. 2, 2017), https://www.reuters.com/article/us-facebook-advertising/facebook-says-10-million-u-s-users-saw-russia-linked-ads-idUSKCN1C71YM.

[22] Robert Booth & Alex Hern, *Intelligence watchdog urged to look at Russian influence on Brexit vote*, The Guardian (Nov. 15, 2017), https://www.theguardian.com/uk-news/2017/nov/15/intelligence-watchdog-urged-to-look-at-russian-influence-on-brexit-vote.

[23] Karla Adam & William Booth, *Rising alarm in Britain over Russian meddling in Brexit vote*, Wash. Post (Nov. 17, 2017), https://www.washingtonpost.com/world/europe/rising-alarm-in-britain-over-russian-meddling-in-brexit-vote/2017/11/17/2e987a30-cb34-11e7-b506-8a10ed11ecf5_story.html?utm_term=.f3a516b9f357.

[24] Laura Daniels, *How Russia hacked the French election*, Politico (Apr. 23, 2017), https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/.

[25] Michael Schwirtz, *German Election Mystery: Why No Russian Meddling*? N.Y. Times (Sept. 21, 2017), https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html.

[26] *Id.*

[27] *Id.*

[28] Jacqueline Williams, *Australian Lawmaker Quits Amid Questions Over China Ties*, N.Y. Times (Dec. 12, 2017), https://www.nytimes.com/2017/12/12/world/australia/sam-dastyari-resigns-china.html?_r=0.

[29] Kelsey Munro, *What is really in Australia's new foreign interference laws?* SBS News (Dec. 8, 2017), https://www.sbs.com.au/news/what-is-really-in-australia-s-new-foreign-interference-laws.

[30] *Id.*

While the specifics of the foreign influence campaign in 2016 may have been difficult to anticipate, the gaps in our campaign finance laws and regulations that allowed this influence were known to the government before the events of 2016 gave them public prominence. For years, as Brendan Fischer describes, Congress and the FEC have failed to update disclosure and disclaimer requirements for the realities of the digital age. These failures created attractive openings for those hoping to interfere with the election, sow discord, and undermine our democracy.

Campaign Finance Law in the 21st Century

By Brendan Fischer

Brendan Fischer directs the Federal and FEC Reform Program at the Campaign Legal Center.

Long-standing U.S. law prohibits any foreign national from financially influencing U.S. elections, whether through direct contributions to candidates or spending any money whatsoever for the purpose of influencing an election.[1]

The law also prohibits anyone from soliciting a contribution or expenditure from a foreign national. And it prohibits any person from "knowingly providing substantial assistance" in the making or solicitation of a foreign national's contribution or expenditure.

Moreover, in contrast with almost every other provision of federal campaign finance law, the foreign national prohibition applies to elections at every level of government: federal, state, and local. This is the broadest prohibition in all of U.S. campaign finance law.

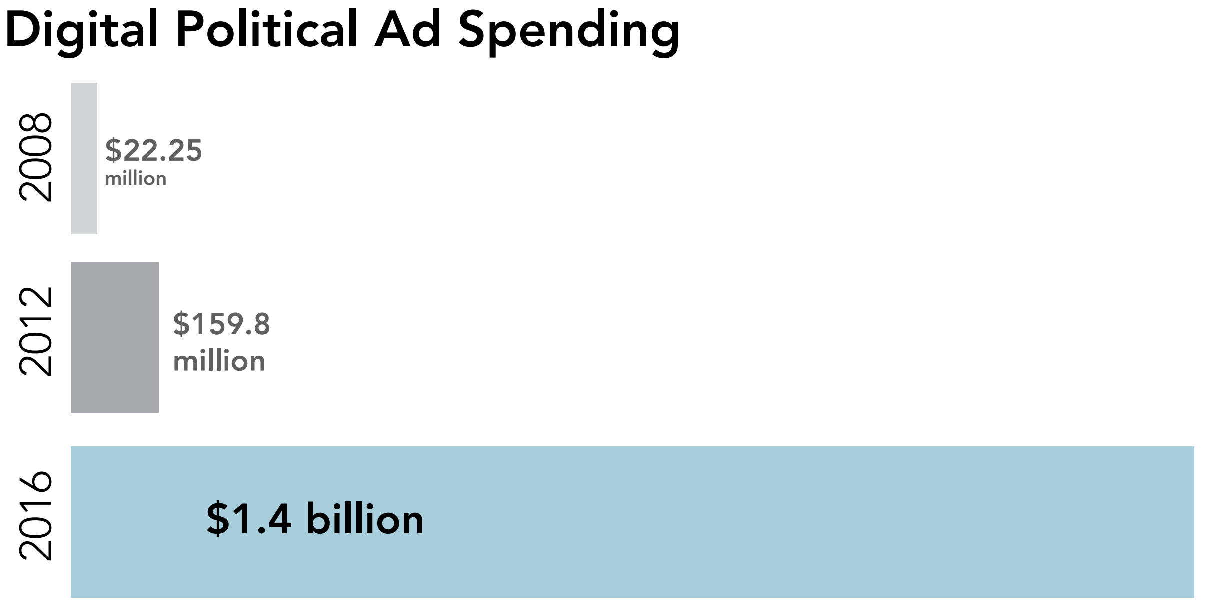
Even as courts have struck down other limits on money in elections, they have upheld the foreign national ban. In 2012, two years after the Supreme Court in *Citizens United v. FEC* dealt a blow to domestic campaign finance laws by striking down the ban on corporate independent expenditures, that same Court summarily affirmed a decision upholding the broad foreign national prohibition in *Bluman v. FEC.* As the D.C. District Court held: "It is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government."[2]

> "It is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government."
>
> - Bluman v. FEC (D.D.C. 2011)

But modern forms of political campaigning have presented unique challenges to the enforcement of the foreign national ban.

Analog Law for the Digital Era

Political campaign activity is migrating to the internet. In 2012, only 1.7 percent of political ads were digital; by 2016, it was 14.4 percent.[3] $1.4 *billion* was spent on digital political ads in 2016,[4] compared to $159.8 million in 2012,[5] and just $22.25 million in 2008.[6]



Source: Borrell Associates

And those numbers are expected to continue growing.

Yet the last major reforms to U.S. campaign finance law came in 2002, in the relative infancy of the web. Since then, thanks in part to lobbying by platforms like Facebook, both Congress and the FEC have largely failed to update laws and regulations as political campaigning has increasingly moved online.

In the 2016 election, Russia secretly exploited these gaps in the law, allowing many illegal communications to circulate, undetected and undeterred.

What were those digital gaps?

First, reporting and disclosure.

"Independent expenditures" are campaign ads that expressly call for the election or defeat of a candidate.[7] Throughout the 1980s and 1990s, however, it became apparent that this definition left open a loophole: Advertisers could evade disclosure requirements with so-called "issue ads" attacking or supporting a candidate but stopping short of express advocacy. To close this loophole, the 2002 reforms created a new category of expenditures called "electioneering communications," defined as ads that name a candidate and are broadcast to the candidates' voters within 30 days of the primary or 60 days of the general election.[8] Electioneering communications are subject to reporting and disclosure requirements once more than $10,000 is spent.[9]

This definition of electioneering communications, however, only applies to broadcast ads—it does not include digital messages.[10] An ad that may be subject to reporting and disclosure when aired on TV can remain shrouded in secrecy when run online.

This means that the loopholes closed for TV in 2002 have remained open for digital ads. And the problems associated with this have become increasingly obvious as more political ad spending migrates online. Of the $1.4 billion spent on online political ads in the 2016 cycle,[11] only a fraction was reported to the FEC.

Russian actors, of course, never disclosed their political ad spending to the FEC—but they were largely not required to do so, and neither were any other similar digital advertisers.

Second, disclaimers.

Disclaimers stating who paid for a political ad are ubiquitous during election season. Political TV and radio ads contain a statement from the narrator declaring the name of the entity that paid for the message. Newspaper ads and mailers must include a box stating the name of the group that bought it.

Digital ads, however, often omit the same "paid for by …" message that usually accompanies political advertisements.

To a significant degree, this is due to the FEC applying 20th century disclaimer exceptions to 21st century forms of political advertising. According to FEC regulations, a disclaimer is not required on an ad that is too small to include it (the rules reference "[b]umper stickers, pins, buttons, [and] pens") or on an ad where including a disclaimer would be impracticable (like "[s]kywriting [and] water towers").[12]

Facebook ads, for example, might be the same size as a lapel pin, but are not subject to the same constraints: Digital ads might fit only a certain number of characters on the ad itself, but, unlike a lapel pin, can readily provide viewers with "paid for by …" information through other means. Yet, through regulations and a series of advisory opinions, the FEC has created ambiguity about when disclaimers are required for online ads—meaning that many ads don't include disclaimers at all.[13]

The Supreme Court has noted that political advertising disclaimers "insure that the voters are fully informed about the person or group who is speaking,"[14] allow voters to "evaluate the arguments to which they are being subjected,"[15] and "enable[ ] the electorate to make informed decisions and give proper weight to different speakers and messages."[16]

It should go without saying that voters would assess a political ad differently if they knew that Russia was behind it. And it does not appear that Russia's secretly sponsored political ads in 2016 included disclaimers. If disclaimers had been required for online political ads, the Russian influence effort might have been uncovered sooner.

The third gap that was exposed in 2016 involved transparency about the ads themselves and about their dissemination.

Under current law, television and radio ads are subject to an additional layer of transparency through a Federal Communications Commission (FCC) requirement that broadcasters make public information about who paid for an ad and how much they spent. No such requirement currently exists for digital ads. And, by their very nature, television and radio ads are widely distributed and the content usually available to the press and public; many digital ads, in contrast, are highly targeted and difficult for anyone other than the targeted recipients to obtain. This is sometimes known as the "dark post" phenomenon.

JUST 3,000 RUSSIAN FACEBOOK ADS REACHED AT LEAST 10 MILLION AMERICANS

Source: Facebook

Taken together, these three online loopholes allowed Russia to secretly purchase thousands of digital political ads that reached potentially hundreds of millions of Americans. This included at least 3,000 political ads on Facebook that reached at least 10 million people,[17] 150 ads on Instagram,[18] and ads on Google, YouTube, Gmail,[19] Twitter,[20] and even Pokemon Go.[21]

Although many of these ads were illegal under existing law, the online transparency gaps described above allowed these messages to circulate, undetected and undeterred.

Had effective online disclaimer and disclosure laws been in place in 2016, Russia's wide-ranging influence campaign might have been detected sooner—or Russia might have been deterred from engaging in the effort in the first place.

A bipartisan group of legislators has introduced a bill called the HONEST Ads Act to shore up these vulnerabilities and close the internet blind spot that allows online political ads to escape the transparency requirements that apply to similar ads run on any other medium.[22]

First, the legislation would expand the definition of "electioneering communications"—and thereby the corresponding disclaimer and reporting requirements—to include paid online ads.

Second, the bill would make online ads that advocate for or against candidates subject to the same disclaimer rules as offline election ads. The Act would also prohibit the FEC from deciding that digital ads are exempt from disclaimer requirements. Even if foreign-funded ads were hidden behind innocuously named entities like "Secured Borders," the disclaimer information would provide additional data points to allow journalists, watchdog groups, or law enforcement to identify foreign actors attempting to surreptitiously influence U.S. elections. As Dana Priest has noted, civil society networks in European countries, for example, have made use of a variety of publicly available data to uncover Russian online influence efforts in those countries.[23] Requiring all online political ads in the U.S. to include disclaimer information could similarly allow Americans to identify foreign influence campaigns.

Third, the HONEST Ads Act would create a recordkeeping requirement for digital ads that is analogous to the requirements that currently only apply to television and radio ads. The bill would require that large platforms like Facebook maintain a digital copy of ads from advertisers whose spending on those ads exceeds a certain amount, and that they collect basic information about the advertisers. As is the case with broadcast ads, this section would apply to both explicit campaign ads and more general political advertising. This would help address the "dark post ad" phenomenon, where highly targeted online ads are never seen by the broader public.

The HONEST Ads Act, introduced with bipartisan co-sponsors in both the Senate and House in 2017, has yet to receive a hearing. But passage of this bill (or one with similar provisions) would create some parity between digital and broadcast ads and close the loopholes Russia exploited in 2016.

Low-Cost Digital Politicking Presents Unique Challenges

Another challenge posed by the shift toward digital campaigning is that federal campaign finance laws are drafted to address paid political activity—and online political campaigning often does not have a price tag.

Campaign finance laws are designed to limit the corruptive influence of money in politics. In many cases, individual volunteer activity does not appear to directly implicate those concerns. For example, federal law does not regulate unpaid volunteers stuffing envelopes at campaign offices or knocking on doors to support a candidate.[24]

When it comes to the foreign national ban, campaign finance law's money-centric approach made sense in an era where reaching voters largely required paying television or radio stations to run ads, or paying a printing shop and the U.S. Postal Service to print and distribute flyers. The law clearly prohibited—and continues to prohibit—foreign nationals from paying for these activities.

But a sizable portion of online foreign influence efforts in 2016 did not involve such obvious expenditures. Although Russia did pay platforms like Facebook for political advertising, Russia also created thousands of *free* fake accounts on social media platforms like Twitter and Facebook to spread election-related messages, to promote hacked material, and, in some cases, to distribute demonstrably false information.[25] Some of those accounts were automated "bots" created to help those messages go viral and reach wider audiences—again, without making any payments to Twitter or Facebook.[26] The low-cost or no-cost nature of social media activity means that little to none of this activity is reported to the FEC or any other federal agency. (See the article from Douglas Guilbeault and Robert Gorwa for further discussion of bots.)

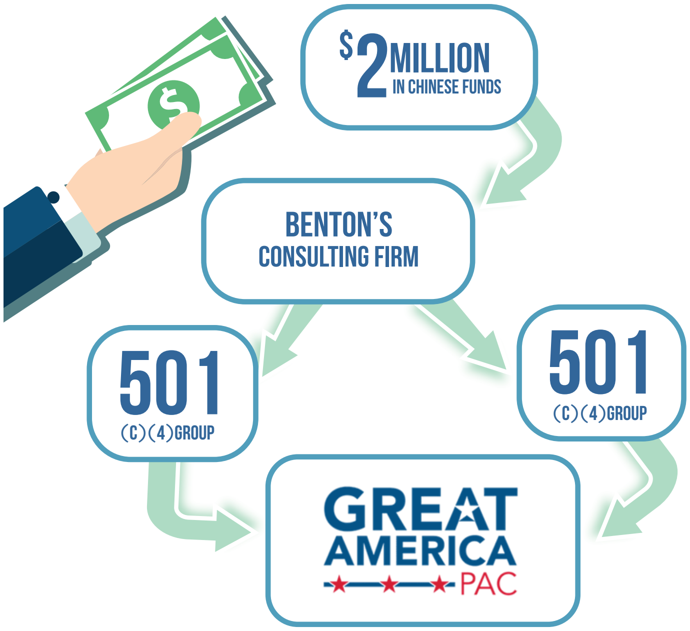
Dark Money Can Hide Foreign Money

Another challenge in enforcing the foreign national ban arises from the difficulty in identifying violations in the first place.

At least $800 million in "dark money" has been spent on U.S. elections since the 2010 *Citizens United* decision, largely by tax-exempt corporations incorporated under Section

501(c)(4) and (c)(6) of the tax code.[27] Because these nonprofit entities keep most or all or their donors secret—and Congress and the FEC have done nothing to close these transparency gaps—there is no way of knowing whether, or to what extent, their funding was derived from foreign sources.

Two underreported examples from the 2016 election illustrate how dark money and corporate contributions can disguise foreign influence.



Source: *The Telegraph*

First, an undercover investigation by U.K. newspaper *The Telegraph* showed representatives of the pro-Trump super PAC Great America PAC offering to help a fictitious Chinese businessman illegally contribute $2 million to the PAC by routing the funds through a for-profit company and two 501(c)(4) organizations.[28] Specifically, a consultant to the super PAC suggested to the undercover reporters that he could help the foreign donor route contributions from the donor to the consultant's consulting firm, then to two 501(c)(4s), and then to the super PAC—leaving no trace that the money had come from a foreign national. The super PAC also promised that candidate Trump would be made aware of the foreign national's secret contribution.

The Great America PAC example shows how dark money corporations can be used to hide foreign money in U.S. elections. Although the plan was illegal, the scheme would likely never have come to light had the conversations not been recorded and publicly released.

Second, more recent reporting has raised other questions about dark money entities hiding foreign funds. For example, the National Rifle Association (NRA) has been building financial relationships with Russian nationals—including government officials—for several years[29]—and the NRA's 501(c)(4) dark money arm, NRA-ILA, spent more than $30 million on 2016 races.[30] Reports that operatives sought to use the NRA's 2016 convention to make "first contact" between the Trump campaign and the Kremlin may raise further questions about whether any foreign funds were part of the NRA-ILA's dark money spending.

A related issue is the role of foreign-owned or -controlled corporations, to which the FEC has given broad leeway to spend money influencing U.S. elections after *Citizens United*.

Under current law, a corporation that is *entirely owned or controlled* by a foreign national is not itself a "foreign national" as long as it is organized under U.S. law and has its principal place of business in the U.S.[31] Some lawyers have advised that foreign-owned U.S. companies may make contributions as long as, among other things, the foreign owners or board members are not involved in the decision-making process.[32]

Yet reporting by *The Intercept* revealed how at least one foreign corporation in the 2016 cycle violated even these narrow provisions.

The Intercept uncovered how a U.S. corporation, American Pacific International Capital, Inc. (APIC), which was controlled by Chinese citizens living in Singapore, gave $1.3 million to Right to Rise, a super PAC supporting presidential candidate Jeb Bush. Existing federal laws and regulations would likely have permitted this contribution if the decision was made exclusively by U.S. nationals—but *The Intercept* discovered that APIC's Chinese owners had directed the contribution, rendering it illegal.

There is every reason to believe that the APIC example is only the tip of the foreign money iceberg. APIC's contribution was identified because it was made to a super PAC and publicly disclosed—allowing *The Intercept* reporters to dig deeper. Any foreign-owned or foreign-controlled corporations that secretly gave to dark money groups, in contrast, are not known. Current laws and regulations present disturbing opportunities for corporations wholly or partially owned by foreigners to legally make contributions to super PACs and dark money groups, as long as they carefully hide this activity.

The desire of foreign governments and other foreign interests to influence U.S. elections and U.S. policy is unlikely to abate.

The loopholes exploited by foreign actors in the 2016 elections are certain to be used again in 2018 and beyond—unless we take action.

[1] 52 U.S.C. § 30121(a).

[2] *Bluman v. Fed. Election Comm'n*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011).

[3] Kip Cassino, *What Happened to Political Advertising in 2016 (and forever)*, Borrell Associates, Inc. (2017).
Even candidates and political committees that file regular reports with the FEC can disguise their overall digital spending. Some committees report direct payments to Facebook or Twitter for advertising, which may not include the detail of an electioneering communication report, but provides some sense of overall spending. But other committees only report lump-sum payments to "digital consultants," who then never report the amount paid to Facebook or other advertisers.

[4] *Id. See also* Kate Kaye, *Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast Down 20%, Cable and Digital Way Up*, AdAge (Jan. 3, 2017), http://adage.com/article/media/2016-political-broadcast-tv-spend-20-cable-52/307346/.

[5] *Id.*

[6] Issie Lapowsky, *Political Ad Spending Online is About to Explode*, Wired (Aug. 18, 2015), https://www.wired.com/2015/08/digital-politcal-ads-2016/.

[7] 52 U.S.C. § 30101(17).

[8] 52 U.S.C. § 30104(f)(3).

[9] 52 U.S.C. § 30104(f)(1-2). Electioneering communication reports describe the amount spent on the ads, the candidates supported or opposed, and the names of contributors who gave for the purpose of furthering the advertisement. *Id.*

[10] 52 U.S.C. § 30104(f)(3)(a)(i).

[11] Cassino, *supra* note 3.
Even candidates and political committees that file regular reports with the FEC can disguise their overall digital spending. Some committees report direct payments to Facebook or Twitter for advertising, which may not include the detail of an electioneering communication report, but provides some sense of overall spending. But other committees only report lump-sum payments to "digital consultants," who then never report the amount paid to Facebook or other advertisers.

[12] 11 C.F.R. § 110.11(f)(1)(i-ii).

[13] *See*, *e.g.*, Advisory Opinion 2010-09 (Google), Advisory Opinion Request 2011-09 (Facebook); *but see* Advisory Opinion 2017-12 (Take Back Action Fund).

[14] *Citizens United v. FEC*, 558 U.S. 310,368 (2010) (internal citations and quotation marks omitted).

[15] *Id*. at 368 (quoting First Nat. Bank of Boston v. Bellotti, 435 U.S. 765, at 792, n. 32).

[16] *Id*. at 371.

[17] Mike Isaac & Scott Shane, *Facebook's Russia-Linked Ads Came in Many Disguises*, N.Y. TIMES (Oct. 2, 2017), https://www.nytimes.com/2017/10/02/technology/facebook-russiaads-.html.

[18] James Rogeres, *Facebook: 150 Russia-Linked Political Ads Showed Up On Instagram*, FOX NEWS (Oct. 9, 2017), http://www.foxnews.com/tech/2017/10/09/facebook-says-150-political-ads-linked-to-russia-showed-up-on-instagram.html.

[19] Elizabeth Dwoskin, Adam Entous, & Craig Timberg, *Google uncovers Russian bought ads on YouTube, Gmail and other platforms*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russianbought-ads-on-youtube-gmail-and-other-platforms/?utm_term=.8c7d310109cf.

[20] Lauren Gambino, *Democrats Rebuke Twitter for 'Frankly Inadequate' Response to Russian Meddling*, THE GUARDIAN (Sept. 28, 2017), https://www.theguardian.com/technology/2017/sep/28/twitter-congress-russian-electioninterference.

[21] Rebecca Savransky, *Russian-Linked Campaign Used Pokemon Go to Meddle in Election*, THE HILL (Oct. 12, 2017), http://thehill.com/policy/technology/355189-russianlinked-campaign-used-pokemon-go-to-meddle-in-election.

[22] HONEST Ads Act, S.1989, H.R. 3077, 115th Cong. (2017).

[23] *See* Dana Priest & Michael Birnbaum, *Europe Has Been Working to Expose Russian Meddling for Years*, WASH. POST (June 25, 2017) https://www.washingtonpost.com/world/europe/europe-has-been-working-to-expose-russianmeddling-for-years/2017/06/25/e42dcece-4a09-11e7-9669-250d0b15f83b_story.html?utm_term=.b9a8f6f209c5.

[24] In fact, the FEC has expressly allowed foreign nationals to volunteer on campaigns or for political committees. *See*, *e.g.*, Advisory Opinion 1987-25 (Otaola); Advisory Opinion 2014-20 (Make Your Laws PAC).

[25] 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?mcubz=0&_r=0

[26] *Id.*

[27] *Outside Spending by Nondisclosing Groups, Cycle Totals, Excluding Party Committees*, Center for Responsive Politics, https://www.opensecrets.org/outsidespending/nonprof_summ.php?cycle=2018&type=type&range=tot (last visited Dec. 13, 2017).

[28] Investigations team & Ruth Sherlock, *Exclusive: Pro-Trump campaign group should face inquiry over 'foreign donor', leading election lawyer states*, The Telegraph (Oct. 25, 2016), http://www.telegraph.co.uk/news/2016/10/25/exclusive-pro-trump-campaign-group-should-face-inquiry-over-fore/.

[29] Rosalind S. Helderman & Tom Hamburger, *Guns and religion: How American conservatives grew closer to Putin's Russia*, Wash. Post (Apr. 30, 2017), https://www.washingtonpost.com/politics/how-the-republican-right-found-allies-in-russia/2017/04/30/e2d83ff6-29d3-11e7-a616-d7c8a68c1a66_story.html?utm_term=.fdadfdb1f936.

[30] *NRA Institute for Legislative Action*, Center for Responsive Politics https://www.opensecrets.org/outsidespending/recips.php?cmte=C90013301&cycle=2016 (last updated Dec. 7, 2017).

[31] *See* 52 U.S.C. 30121(b) (citing 22 USC 611(b)).

[32] *See, e.g.*, Memo from Charlie Spies to Right to Rise super PAC, "Contributions By Domestic Subsidiaries of Foreign Corporations to Federal Super PACs" (Feb. 19, 2015), https://theintercept.com/document/2016/08/03/right-to-rise-usa-memo-on-foreign-owned-corporations-donating-to-super-pacs/. *See also* MUR 6401/6432 (Transcanada) (FEC enforcement action concluding that contributions to Nebraska state candidates by the U.S. subsidiary of a foreign corporation, Transcanada, were permissible because the funds were derived from U.S. revenue and all decisions were made by a U.S. citizen.) Federal law's foreign national prohibition was crafted in a pre-*Citizens United* world, where corporations were barred from spending money in elections. The statute does not reference corporations; instead, it cross-references definitions in FARA, which provides that a corporation wholly or partially owned or controlled by a foreign national is not itself a "foreign national," as long as it is organized under U.S. law and has its principal place of business in the U.S. *See* 52 U.S.C. 30121(b) (citing 22 USC 611(b)).

Many Americans were hardly aware of "bots" before the 2016 election. But they are omnipresent on social media networks: According to one study, as many as 15 percent of Twitter accounts could be automated bots, which, based on Twitter's 313 million active users, means the number of bots could be between 28 million and 47 million.[1] Should bots be regulated to prevent their misuse by foreign actors? Douglas Guilbeault and Robert Gorwa address how the rise of automated online and social media activity presents new challenges for regulators and social media companies themselves.

Current Challenges for Bot Policy and Foreign Interference

By Douglas R. Guilbeault and Robert Gorwa

Douglas Guilbeault is a researcher in the Network Dynamics Group and a Ph.D. candidate at the University of Pennsylvania's Annenberg School for Communication. He is an affiliated researcher of the ComProp project at the Oxford Internet Institute and the Digital Intelligence Lab at the Institute for the Future.

Robert Gorwa is a Ph.D. student in the Department of Politics and International Relations at the University of Oxford. He conducts research on political bots with the ComProp project at the Oxford Internet Institute.

The 2016 election has demonstrated that the automation policies of platform companies can have a substantial public and political impact. Amidst mounting concern about digital influence operations conducted via social media, Facebook and Twitter have been called to testify before Congressional Intelligence Committees about bots and foreign influence during the 2016 election, and have been pressed to discuss proposed solutions for addressing the issue.

In this report, we discuss the complex challenges for policymakers and scholars concerned by the threat of foreign interference via automated social media accounts. We outline how the current landscape of "bot policy" is characterized by broad ambiguity as to what exactly constitutes a bot, as well as how these bots should be detected, classified, measured, and governed. Most critically, we suggest that initiatives put forth by policymakers or deployed by social media companies will have to deal with challenges that can be divided into three critical areas: ambiguity, legitimacy, and responsibility.

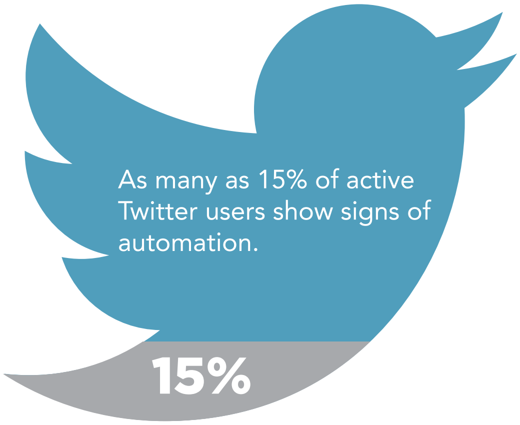
Ambiguity

The first challenge for policymakers and researchers interested in bots is that from its very origins, the term "bot" has been highly ambiguous. Although it has become a commonly used term, it has yet to crystallize into a discrete or coherent concept. During the early days of personal computing, the term was employed to refer to a variety of different software systems, such as daemons and scripts that would send warning messages or update notifications to people as they operated their computers.[2] Categorically different types of software, such as early programs that deployed procedural writing to converse with a human user, were branded chatbots (but often also called bots). In the 2000s, "bot" developed an entirely new series of associations in the network and information security literatures. In this literature, bots refer to computers compromised, co-opted, and remotely controlled by malware, where these devices can be linked in a network (i.e., a "botnet") used to carry out distributed denial of service (DDoS) attacks.[3] During the rise of Twitter and Facebook, automated social media accounts began to be known as "bots."[4] These automated accounts are generally the type of bot that is the focus for policymakers and researchers today.

However, a huge variety of terminology has emerged, and, confusingly, is often used interchangeably by academics, journalists, and policymakers: robots, bots, chatbots, spam bots, social bots, political bots, botnets, sybils, sockpuppets, and cyborgs seem to refer to everything from automated social media accounts to recommender systems and web scrapers. Equally important to these discussions are terms like trolling, troll farms, and astroturfing, which need not involve automation at all, though they are also occasionally described as being performed by bots. Bots are predominantly described as negative or malicious, with research highlighting how they can be used to game algorithms and recommender systems[5], stifle[6] or encourage[7] political speech, and help circulate hyperpartisan "fake news."[8] But different types of automated accounts have also been deployed on platforms to, for example, facilitate greater participation on behalf of minority voices. Savage et al.'s Botivist system (merging bot and activist) tweets out calls to action concerning corruption in Latin America.[9] In initial demonstrations, over 80 percent of people responded to Botivist's calls to action, and they responded with effective proposals for how to address the assigned social problem. Other bots, such as the @StayWokeBot on Twitter, or the New York Times bot on Facebook, encourage civic participation and spread news about important social movements. A recent experiment also demonstrates how, under tightly controlled experimental conditions, bots can be used to systematically enhance coordination in large social networks.[10] It is clear that bots—conceived generally as automated communicative systems on social media—are not inherently "bad."

This is a fundamental challenge for both the platform companies and for policymakers: How can the use of positive, democracy and community-enhancing automation be encouraged, while also preventing its use for political manipulation, astroturfing, deception, and other various developing forms of online abuse?

Other problems stem from this lack of clear understanding as to what exactly "bots"—especially when used for foreign interference—look like. When Twitter and Facebook make public statements about bots, for example, the assumption is that bots refer to a kind of political automation that operates over these social media platforms. However, among the journalists and researchers who served to raise attention about bots, the term bot is used to refer to many different online actors, and the infamous "Russian bots" may not be automated at all, but seem to also refer to manually controlled accounts



Source: Onur Varol et al.

as well. This especially is reflected in one of the major issues for bot scholars: the difficulty of understanding and categorizing hybrid forms of automation. Accounts that have both human and automated characteristics have been referred to as "cyborgs," but these accounts present a major challenge as they do not follow patterns otherwise established as indicators of potentially automated activity.[11]

Another emerging trend of digital manipulation involves humans volunteering their personal accounts to be automated for a broader, political purpose. One example involved a group of young activists who volunteered their accounts on Tinder—a social media dating app—to be used by a bot to target voters in swing districts during the United Kingdom's 2017 snap election.[12] While this kind of activity is currently the exception, not the norm, it will pose even more significant challenges for detection and for formulating coherent concepts of what exactly bots are. Twitter and Facebook currently lump the full spectrum of bot-related activity into a category of "suspicious or malicious" users, as distinct from "good" users or "good" automation, a dichotomy that is problematized by users who volunteer their authentic profiles to be automated for a cause.

Therefore, the idea of measuring bot effects becomes ambiguous. There are reasons to think there are technical limitations in the platforms' own ability to detect bots with confidence. Facebook has admitted that its platform is so large that accurately classifying and measuring activity by malicious actors is a major challenge. But detecting bots and measuring foreign influence is an even larger challenge for researchers, who do not have access to critical data.

For example, the policy implications of this challenge become very apparent in the context of the recent debate over pages spreading inflammatory political content during the 2016 U.S. election. While Facebook initially claimed that only a few million people saw advertisements that had been generated by these pages, a researcher at Columbia used Facebook's own advertising tools to track the organic reach that these posts had generated, concluding that they had been seen "hundreds of millions of times."[13] However, others suggested that these views were created by illegitimate automated accounts. However, it is impossible for researchers to verify how many people actually saw this content, and indeed, it is not currently possible—given the data access provided by companies like Facebook—for researchers to either discount or accurately measure the possibility that indicators such as likes and shares are being artificially inflated. To understand the scope and scale of the problem, policymakers will need more reliable indicators and better measurements than are currently available, and, indeed, measurement ambiguities are among the most pressing challenge for bot policy moving forward.

To understand the scope and scale of the problem, policymakers will need more reliable indicators and better measurements than are currently available.

Incentives

This dichotomy between positive and negative forms of activity is also a key policy challenge. Underpinning Twitter's policy statements is the belief that Twitter can clearly distinguish "good" from "bad" uses of automation.[14] As Twitter has long encouraged automation by providing an open application programming interface (API) with very permissive third-party application policies, automation drives a significant amount of traffic on this platform.[15] Twitter allows accounts to easily deploy their own applications or use tools that automate their activity, which can be useful: Accounts run by media organizations, for example, can automatically tweet every time a new article is published. This decision to preserve a place for bots in social media is due, in part, to the fact that Facebook and Twitter have vested interests in hosting "legitimate" types of activity: Both social networks appeal to shareholders by calculating their "total monthly active users." Social bot accounts can inflate these numbers, and their activity may also influence recorded click rates on digital advertisements, which are used to sell digital real estate.[16]

These incentives are critical in shaping bot policy for the social media companies. For example, while Twitter's core concern is with increasing traffic, Facebook has been battling different types of invasive spam for years and has much tighter controls over its API. As such, it appears that Facebook has comparatively much lower numbers of automated users, but, instead, is concerned primarily with manually controlled sockpuppet accounts.[17] For both companies, delineating what is legitimate and illegitimate activity will be a key issue. Twitter would certainly prefer to be able to keep its legitimate and benign forms of automation (bots that tweet the weather every day, for example) and only clamp down on malicious automation. But doing so is difficult, as the same processes enable both types of activity.

Meaningful changes would require reimagining Twitter's core philosophy as an open platform and would likely require the social network to institute some kind of approval system for third-party applications.[18] For Facebook, redesigning the platform to reduce political automation runs against new complexities stemming from the platform's private format. A "privately formatted" social media platform refers to a platform where user profiles and group communication mechanisms (e.g., Facebook's "News Feed") are not, by design, open to the global public, but are, rather, confined to the social network a user privately builds. Facebook's private nature makes it more resilient to bot interference, but not impervious. As such, Facebook demonstrates that making social media networks more private is not sufficient to protect against bots. In fact, Facebook's private nature enables users to grow biased social networks of like-minded peers—often called "echo chambers"— which are highly susceptible to the automated spread of misinformation and polarizing content.[19] There is a critical need to assess how private versus public social media platforms are impacted by political automation, and whether there is a critical balance in private and public information flow that is optimally resistant to automated deception.

While Twitter generally describes its API constraints in purely technical terms, by defining rate limits on the number of messages an account can produce each day and on the number of accounts that can be associated with single email accounts and IP addresses, Wikipedia, by contrast, defines its API regulations on bots within a framework of Asimovian-esque principles for determining whether a bot can exhibit harm to the community and whether or not it may bring productive contributions to that community.[20] Wikipedia demonstrates that it is possible, given a differing set of goals and incentives, to design community-focused automation policies that have ethical and normative judgments built into them.

While the API regulations from one platform may speak to the other, substantial work is required to better understand how models of bot policy from various platforms could inform or improve the policies of other social networks. In the meantime, policymakers should be mindful of these issues and ensure they do not lose sight of the prospective harms that could accompany inelegant "solutions" to their concerns.

Responsibility

Most bot policy to date has, in effect, followed a self-regulatory approach on behalf of social media companies, who understandably are the primary actors in dealing with content on their platforms, and who manage automation based on their own internal policies. However, the events of the past year have demonstrated that these policies can have serious political ramifications that reach beyond the narrow interests of the platforms, potentially placing these issues more squarely within the realm of regulatory and legal authorities. A key, and unresolved, challenge for policy is the question of responsibility, and the interrelated questions of jurisdiction and authority. To what extent should social media companies be held responsible for the dealings of social bots? And who will hold these companies responsible?

> To what extent should social media companies be held responsible for the dealings of social bots? And who will hold these companies responsible?

While the public debate around automation policies is only nascent at best, it is clearly related to the current debates around the governance of political content and hyperpartisan "fake news." In Germany, for instance, there has been substantial discussion around newly enacted hate-speech laws that impose significant fines against social media companies if they do not respond quickly enough to illegal content, terrorist material, or harassment.[21] Through such measures, certain governments are keen to assert that they do have jurisdictional authority over content that their citizens may be exposed to, especially once the stakes are high enough.

A whole spectrum of regulatory options under this umbrella exists, with some being particularly troubling. For example, some have argued that the answer to the "bot problem" is as simple as implementing and enforcing strict "real-name" policies on Twitter—and making these policies stricter for Facebook. This debate is not a new one—following the so-called "nymwars" of 2011, where users using pseudonyms on the newly founded Google Plus social network had their accounts deleted, scholars including Boyd[22] and Hogan[23] forcefully argued that pseudonymity and anonymity are integral features of modern social networks, and that they afford a whole spectrum of positive and creative behavior. Whether they be youth trying to better understand their sexuality or activists voicing their dissent in repressive regimes, many have benefited from online pseudonymity and anonymity.[24] But, simultaneously, anonymity can be abused by sockpuppets and automated fake accounts that spread hyperpartisan vitriol and play a significant role in disinformation campaigns. What exactly is the appropriate balance?

Another major concern is that governments and corporations can take advantage of ambiguity of bots to advance potentially harmful, and even manipulative, practices. Consider the collaboration between Facebook and the government of Vietnam, where efforts to censor and remove “false” accounts have been accused of being a veiled attempt to censor dissidents.[25] We need to be careful that social media companies and related parties do not define bots in such a vague way that it allows them to essentially remove any user account suspected of demonstrating politically undesirable behavior.

In a sense, technology companies have already admitted at least some degree of responsibility. In a statement issued after Facebook found evidence that Russian-linked groups had purchased political advertising through Facebook’s marketing tools, CEO Mark Zuckerberg claimed that Facebook takes political activity seriously and was “working to ensure the integrity of the [then upcoming] German elections.”[26] Bot policy now matters more than ever, and the automation policies of platform companies can have real political impact. But what should regulators, policymakers, and consumers do?

Possible Solutions

Given the challenges outlined above, three main courses of action are likely to address key issues in bot policy.

First, major progress can be made by carefully distinguishing which elements of bot policy should be within the control of government, and what should be left to self-regulation. The concern with self-regulation is that it often goes hand in hand with a lack of transparency. Significant progress can be made by requiring social media companies to provide detailed reports about their internal bot reviews, and also by requiring social media companies to provide greater access to data on behalf of nonbiased, third-party researchers who can assess the impact of bots on their platform without the conflicting financial incentives that social media companies carry. These reports should not only involve records of how many bots, foreign and domestic, these companies believe are on their platforms, but also reports about how much money these companies make from the rising bot industry, as well as whether these bot accounts significantly interfere with ad revenue and the circulation of news content.

Second, social media companies can learn from websites like Wikipedia, which have clear and accessible public statements about their bot policy[27] and allow decisions about automated accounts to be made by the community. Large social media platforms, however, fall short of facilitating genuine democratic participation when determining key content policies in general, and user populations are entirely left out of the conversation for what kind of content or speech should be allowed on the platforms. Through crowdsourcing mechanisms and public forums, users could be empowered not only to learn about bots and other forms of social and political automation, but also to have a voice in the kinds of content that they wish to permit on the platforms that they use. Public access to this information, coupled with a sense of participation in the structure of their social life online, could make significant contributions to clarifying the bot issue, but would require a complete ideological shift in how Facebook and Twitter conceive of their “community” and the relationships between the companies and their users.

Third, companies can make much greater efforts to strengthen public APIs to prevent bot access. Twitter’s laissez-faire API policies are largely responsible for the proliferation of bots over the platform. Twitter could make it much for difficult for developers to deploy automated accounts, and, for example, require new, unverified applications to go through a simple screening process. This could allow news organizations and other public interest groups to still use automation, while meaningfully reducing the ability of malicious actors to undertake coordinated, automated influence campaigns.

Another critical avenue of intervention involves undertaking a thorough investigation of the funding apparatus involved in purchasing and deploying automated accounts for political purposes. Active research is needed into the political actors spending money on bots, both within the U.S. and abroad. Essential to this inquiry is the rise of "black PR" firms, such as Cambridge Analytica and Deeproot—i.e., organizations that are funded to use machine learning and data analytics to give political operatives a leading edge on the capacity to shape public opinion before major political events.

With this data, regulation could then be developed for the purpose of limiting foreign (and domestic) digital influence operations, and for requiring transparency regarding bots and digital campaigning tactics more generally.

[1] Onur Varol et al., *Online Human-Bot Interactions: Detection, Estimation, and Characterization*, ICWSM (2017), https://arxiv.org/pdf/1703.03107.pdf.

[2] Andrew Leonard, Bots: The Origin of the New Species (1997).

[3] Tyler Moore & Ross Anderson, *Internet Security*, *in* Oxford Handbook of the Digital Economy 572 (Martin Peitz and Joel Waldfogel eds., 2012).

[4] Samuel C. Woolley, *Automating Power: Social Bot Interference in Global Politics*, 21 First Monday (2016).

[5] *Id.*

[6] Emilio Ferrara et al., *The Rise of Social Bots*, 59 Communications of the ACM 96 (2016).

[7] Saiph Savage et al., *Botivist: Calling Volunteers to Action Using Online Bots*, 19th ACM conference on Computer-Supported Cooperative Work and Social Computing (2015).

[8] Chengcheng Shao, *The spread of fake news by social bots*, arXiv:1707.07592 [physics] (July 24, 2017).

[9] Savage et al., *supra* note 7.

[10] Hirokazu Shirado & Nicholas A. Christakis, *Locally noisy autonomous agents improve global human coordination in network experiments*, 545 Nature 370 (2017).

[11] Ferrara et al., *supra* note 6.

[12] Robert Gorwa & Douglas Guilbeault, *Tinder nightmares: the promise and peril of political bots*, Wired (July 7, 2017), https://www.wired.co.uk/article/tinder-political-bots-jeremy-corbyn-labour.

[13] J. Albright, *Itemized Posts and Historical Engagement: 6 Now-Closed FB Pages*, Tableau Public (2017), https://public.tableau.com/profile/d1gi#!/vizhome/FB4/TotalReachbyPage.

[14] Twitter PublicPolicy, *Update: Russian Interference in 2016 US Election, Bots, & Misinformation*, Twitter (Sept. 28, 2017), https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

[15] Zi Chu, *Who is tweeting on Twitter: human, bot, or cyborg*, Proceedings of the 26th Annual Computer Security Applications Conference (2010).

[16] Antonio Garcia Martinez, Chaos Monkeys (2016).

[17] Jen Weedon et al., *Information Operations and Facebook*, Facebook (Apr. 27, 2017), https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[18] Robert Gorwa, *Twitter has a serious bot problem, and Wikipedia might have the solution*, Quartz (Oct. 23, 2017), https://qz.com/1108092/twitter-has-a-serious-bot-problem-and-wikipedia-might-have-the-solution/.

[19] Michela Del Vicario et al., *The spreading of misinformation online*, 113 PNAS 554 (2015), http://m.pnas.org/content/113/3/554. *See also* Pranav Dandekar et al., *Biased assimilation, homophily, and the dynamics of polarization*, 110 PNAS 5791 (2013), http://m.pnas.org/content/110/15/5791.abstract.

[20] Gorwa, *supra* note 17.

[21] Heidi Twoerek, *How Germany Is Tackling Hate Speech*, Foreign Affairs (May 16, 2017), https://www.foreignaffairs.com/articles/germany/2017-05-16/how-germany-tackling-hate-speech.

[22] Danah Boyd, *The politics of real names*, 55 Communications of the ACM 29 (2012).

[23] Bernie Hogan, *Pseudonyms and the Rise of the Real-Name Web*, SSRN (Dec. 1, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229365.

[24] Boyd, *supra* note 21.

[25] Netizen Report Team, *Netizen Report: Vietnam Says Facebook Will Cooperate With Censorship Requests on Offensive and "Fake" Content*, Global Voices (2017), https://globalvoices.org/2017/05/04/netizen-report-vietnam-says-facebook-will-cooperate-with-censorship-requests-on-offensive-and-fake-content/.

[26] Mark Zuckerberg, *I just went live*, Facebook (Sept. 21, 2017), https://www.facebook.com/zuck/posts/10104052907253171.

[27] Gorwa, *supra* note 17.

Prosecuting violations of campaign finance law's foreign national ban and other laws prohibiting "collusion" presents a number of challenges. The ongoing investigation by Special Counsel Robert Mueller has illuminated a number of these challenges, as Daniel A. Petalas describes.

Foreign Interference in Federal Elections: Criminal Tools and Vulnerabilities

By Daniel A. Petalas

Daniel A. Petalas is an owner in the Washington, D.C., office of Garvey Schubert Barer. He is the former acting general counsel and head of the Federal Election Commission's Enforcement Division and a former federal corruption prosecutor at the U.S. Department of Justice.

Since the 2016 election, the Office of the Special Counsel has brought criminal charges against several members of the campaign and administration of President Trump. Each charge is related in some way either to the defendants' Russian-related business activities or false statements to the FBI in its criminal probe of possible cooperation between the campaign and Russian agents in the 2016 election.

At the time of this writing, none of these prosecutions includes charges for involvement in the Russian interference scheme itself. Indeed, few federal statutes criminalize that sort of activity directly. Rather, prosecutors must look to offenses developed to combat the means by which more traditional financial crimes and criminal enterprises operate. To be sure, the government has a variety of tools at its disposal to target certain aspects of a foreign interference campaign. But the difficulties associated with reaching core conduct remain an impediment to effective criminal prosecution and deterrence. Given the intelligence assessment of the 2016 election and the likelihood that foreign intrusion efforts will continue, Congress should consider shoring up gaps that are now evident in the law. The following provides a brief synopsis of some of the potentially applicable theories of prosecution and a few observations about hurdles and vulnerabilities in the present state of the law.

Congress should consider shoring up gaps that are now evident in the law.

1. Offenses Directed at Illegal Foreign Entanglements

At the outset, the crime of treason may seem to apply where a domestic actor assists a foreign power in an attempt to interfere with or obstruct a federal election. The offense proscribes not only levying war against the United States, but also providing an enemy "aid and comfort."[1] It is the most serious offense against the United States, punishable by death, and under the Constitution requires specific and exacting proof to establish. It applies by its terms only to United States citizens.

While the idea of a citizen who owes fidelity to the interests of the United States coordinating with agents of a foreign power to interfere in the democratic process of a federal election suggests disloyalty to the domestic interest, the heightened intent and conduct requirements needed to prove treason make it an unlikely candidate for prosecution absent the most compelling evidence of intentional betrayal. Moreover, at least according to some legal scholars, the meaning of the term "enemy" in the constitutional description of treason further limits prosecution only to assistance of a foreign power that is in open and armed hostilities with the United States. In other words, a betrayal of the domestic interest to a diplomatic or "cold war" adversary may not constitute treason at all as a legal matter.

A related set of offenses, the espionage statutes, is also fairly limited in application here. Espionage focuses on mishandling, revealing, or improperly accessing national security information. But an effort to assist a foreign power in an influence campaign directed at the federal election process, even through an illegal intrusion into private computer systems, need not involve national security information in any respect.

A variety of other offenses directly address activities with foreign governments and their agents, such as the Logan Act and the Foreign Agents Registration Act (FARA), violations of which may be criminally prosecuted. But, again, each is limited to specific conduct that may not reach the foreign influence campaign or its participants.

The Logan Act, for instance, relates to efforts by U.S. citizens to engage with a foreign power to seek to resolve a dispute to which the United States is a party. The statute would likely be subject to constitutional vagueness challenges as applied, and in any event will only reach the aspects of a foreign influence campaign that involve a pointed engagement between a domestic actor and the foreign government on a particular question, such as an effort to alter a sanctions regime against the foreign government, for instance.

As noted, FARA may also have some application. That statute requires a domestic person who serves an as agent of a foreign principal in a political or quasi-political capacity to register with the Department of Justice and disclose that relationship along with that person's activities, receipts, and disbursements.[2] If discovered, the failure to register and disclose can result in prosecution under FARA or as the basis for a false statement prosecution. Indeed, violations of the FARA provisions were among the charges for which Paul Manafort and Richard Gates were indicted by the Office of the Special Counsel. Nonetheless, that statute covers domestic agents, usually paid, who engage in particular undisclosed conduct—political consulting or advocacy directed at Congress or a segment of the U.S. population. As such, it likely exempts as much as it covers when it comes to the overall foreign effort to interfere in the electoral process.

Of perhaps most direct application, the federal campaign finance laws prohibit coordination between a federal candidate's campaign and foreign actors. The Federal Election Campaign Act (FECA) and its amendments bar foreign nationals from spending any funds, directly or in-kind, in connection with any election, whether local, state, or federal. The reciprocal is also true: Candidates, committees, or their agents are prohibited from soliciting, accepting, or receiving a contribution—that is, anything of value—from a foreign national. And solicitation is defined broadly as "to ask, request, or recommend, explicitly or implicitly, that another person make a contribution, donation, transfer of funds, or otherwise provide anything of value." Indeed, soliciting is illegal without regard to whether it actually causes a foreign national to provide any benefit to the campaign. The campaign finance laws also prohibit efforts to disguise foreign involvement through the use of nominee entities or straw donors. Each of these provisions is subject to criminal prosecution if violated, carrying up to five years in prison or a $250,000 fine for a felony conviction.

Nonetheless, campaign finance violations are difficult to prosecute. The FECA creates a dichotomy between non-willful violations of the campaign finance laws and knowing and willful violations. The former are expressly subject to the exclusive jurisdiction of the Federal Election Commission, an independent civil regulatory agency with limited enforcement authority. Only knowing and willful violations may be pursued criminally by federal prosecutors. A knowing and willful violation requires proof, here beyond a reasonable doubt, that the defendant acted with knowledge that the conduct was prohibited by law. In other words, ignorance of the law is a defense to this sort of prosecution. Moreover, if the benefit solicited by an agent of a federal candidate is merely information, there may be room for dispute over whether information can constitute a "thing of value." That said, the term is used in many other criminal offenses and defined broadly to cover all sorts of items, tangible and intangible. Courts have looked to the value the parties place on an item, notwithstanding whether there is any commercial market value.

2. Computer Intrusion Offenses

At least one crime is facially apparent in the 2016 Russian interference campaign. We know that the computer systems of the DNC and the campaign manager of a presidential candidate were illegally accessed. Under the Computer Fraud and Abuse Act (CFAA), it is a five-year federal felony offense to access or conspire to access any computer used in interstate commerce with intent to defraud, if that access furthers the fraud and results in obtaining anything of value.[3] And it seems apparent that troves of pilfered emails and attachments of a competing political campaign would be viewed as things of value, given the competitive value of that information to opponents in a presidential election contest. Thus, the foreign hackers who intruded into those systems would be susceptible to prosecution in the United States, assuming they could be identified or obtained. Further, anyone within the United States who conspired with them, served as an accessory, or sought to obstruct the investigation into their efforts is equally exposed to prosecution.

> Anyone within the United States who conspired with them, served as an accessory, or sought to obstruct the investigation into their efforts is equally exposed to prosecution.

Depending on the facts, the timing of events can be a significant roadblock to charging any domestic individual involved in the presidential campaign under the criminal statutes that relate to computer fraud. In the 2016 election, for example, both the DNC and the John Podesta breaches appear to have occurred before any in President Trump's circle would have been aware of them, at least based on currently available public information. The DNC hack apparently occurred in 2015 and continued through spring 2016, while Podesta was hacked in March 2016. The activity prohibited under the CFAA is complete upon securing illegal access. And, ordinarily, a conspiracy ends upon achievement of its stated purpose (or disbanding of the effort). Thus, even if there were evidence that domestic actors knowingly took advantage of the materials obtained as a result of the illegal access, it is not clear as a legal matter that they can be charged with joining that already completed "computer access" conspiracy—unless, perhaps, there are facts showing that the foreign efforts to access the same or additional covered computer systems in furtherance of the same conspiracy continued after the domestic participants joined it. For example, it has been reported that Russian-related agents continued in their efforts to intrude on the presidential election by targeting nearly two dozen states' computer election systems well after the initial intrusions became public in June 2016, which suggests that the overarching influence campaign, using various actors and processes, remained ongoing.

3. Movement and Concealment of Funds

More broadly, many federal offenses address the methodology involved in criminal activity, and any of those could apply to a foreign influence campaign if triggered. If funds were involved, the movement and concealment of funds in the United States or through other countries could potentially support money laundering, structuring, or related tax charges. Of course, if all funding associated with the influence campaign occurs outside the United States, and assuming any domestic participants assisted without receiving funds or payment, the availability of these theories is of limited use, unless there is a basis to argue that the domestic collaborators conspired or assisted others who did engage in prohibited offense conduct. Again, these tools, robust as they may be in the investigation of traditional frauds, can only reach the conduct that falls within their scope. This is not necessarily the case with a foreign election influence campaign, even if U.S. citizens provide knowing, but unfunded, assistance.

4. Conspiracies and Accessories

A conspiracy to defraud the United States can be demonstrated in two ways.

A conspiracy to defraud the United States can be demonstrated in two ways: by proving an agreement to violate another federal criminal statute or by charging an agreement to impede, obstruct, or interfere with the functions of a component of the federal government. As to a foreign government's effort to influence an election, a conspiracy charge of the first type might stem from any agreement by two or more participants to engage in conduct that violates any of the above-described federal offenses. In this, it is noteworthy that the government is not required to prove that the members of an alleged conspiracy were successful in achieving any or all of the objects or goals of the conspiracy. The mere forming of the agreement to violate a federal law is sufficient.

The other type of conspiracy charge relates to agreements to impede the lawful functions of the federal government. The Supreme Court long ago concluded that it is a conspiracy to defraud the United States to agree to interfere with or obstruct one of the federal government's lawful governmental functions by deceit, craft, trickery, or other dishonest means. As to the 2016 presidential election, however, it is not clear that a presidential election constitutes a function of the federal government. In 1917, the Supreme Court held that conspiring to bribe voters in a *congressional* election does not qualify as conspiracy against the *United States*.[4] This is so, the Court reasoned, because the electoral process has been reserved from the federal government to the several states. Whether the inclusion of the electoral college in the presidential election process distinguishes that holding is an open question. That said, it is a question that Congress can readily fix going forward by expressly identifying an election to federal office as a federal function for purposes of certain specific sections of the criminal code, such as the conspiracy and mail- and wire-fraud statutes.

Absent a conspiratorial agreement, a person may also be liable as an accessory if he knows that an offense was committed and assists the offender with the specific intent or design of hindering or preventing the offender's apprehension, trial, or punishment. However, taking advantage of the fruits of a crime does not make one an accessory. Nor does merely standing silent and not revealing the existence of another's crime. The focus is on the active effort to aid and conceal the offender's known wrongdoing. And although some may take steps to conceal their own involvement at various stages, potentially in violation of the false statement or obstruction of justice statutes, to prove liability under an aiding and abetting or accessory theory, the government needs evidence from which to draw an inference, beyond a reasonable doubt, that the alleged accessory harbored an intent to hinder another known offender's prosecution and took some active step in the effort to do so.

5. False Statements and Obstruction

Finally, the obstructive conduct that often follows activities that, whether illegal or not, those involved would rather not see exposed provides a variety of additional theories of prosecution—perhaps the most fertile soil in cases involving alleged public corruption or, as here, assisting a foreign influence campaign.

It is a felony offense to knowingly and willfully make a materially false statement or representation in most matters within the jurisdiction of the executive or legislative branches of the federal government, such as an FBI or congressional investigation. A false statement is material if it has the natural tendency to influence or is capable of influencing the body to which it is addressed. This is a multipurpose tool of broad application to prosecutors. In a case that involves political campaigns and public officials and multiple federal and congressional investigations, prosecutors will carefully scrutinize the numerous potential applications of the false statements offense to the broad scope of conduct it covers. For example, false statements made in certified submissions outside the investigation itself—on national security forms, federal employment paperwork, vetting materials submitted to Congress by nominees, or the myriad federal filings necessary to conduct business or move money—all may be subject to the reach of the federal false statement offense. Moreover, evidence that an individual "colluded" with a foreign government in an influence campaign, even if not prosecuted under some other criminal theory, can demonstrate the intent with which omissions or errors in other filings to the federal government were made, thus providing the government with evidence to defeat a defense that the error or omission was an oversight and not willful.

Similarly, the obstruction of justice statutes cover a broad range of potentially prosecutable conduct in covering up even lawful associations with a foreign influence effort. The offense of obstruction criminalizes attempts to obstruct, impede, or corruptly influence proceedings, whether successful or not. This can also include proceedings that are merely foreseeable, even if they have yet to commence. The government will rely upon the entire course of conduct, including any relevant background evidence—again, such as proof of collusion, even if not charged under some other criminal theory—as proof of the necessary element of "corrupt" intent on which a conviction under an obstruction theory will depend. In this, among the more significant facts will be evidence reflecting efforts to conceal conduct, engage in private conversations, destroy evidence, or circumvent reporting requirements. Nonetheless, proving beyond a reasonable doubt that an actor took steps that could impede an investigation with the necessary corrupt motive is no easy task, especially where the steps are lawful in themselves and subject to other explanations.

Despite the number of criminal statutes possibly touching on a foreign influence campaign, on review it appears that the most plausible theories of prosecution are potential campaign finance-related and false statement or obstruction theories of liability. But Congress could resolve some of those difficulties as applied in future election cycles with the stroke of a pen, by defining a federal election as a federal function for purposes of certain specified criminal statutes.

The most plausible theories of prosecution are potential campaign finance-related and false statement or obstruction theories of liability.

[1] 18 U.S.C. § 2381.

[2] 22 U.S.C. § 612(a).

[3] 18 U.S.C. § 1030.

[4] *United States v. Gradwell*, 243 U.S. 476 (1917).

U.S. laws are only one element of efforts to protect the sovereignty of our democracy and limit foreign interference. U.S. foreign policy also plays a critical role in deterring election meddling on the international stage. However, as Max Bergmann argues, those protections appear to have failed in 2016.

America's First Line of Defense May Have Failed in 2016

By Max Bergmann

Max Bergmann is a senior fellow at the Center for American Progress. He served in the U.S. Department of State from 2011 to 2017.

Deterrence may have failed during the 2016 election.

America's first line of defense against a foreign country intervening in its elections is not America's legal system, but an awareness on the part of other nations that doing so could have massive repercussions. Simply put, intervening in a U.S. election would have huge costs that would presumably outweigh the benefits of intervention.

What country would dare risk the ire of the United States of America by intervening in one of its elections?

Now we know. In 2016, deterrence failed. Russia not only intervened in the election through an unprecedented information operation focused on social media, but also by seeking to hack into the architecture of registration and voting systems.

Russia did this in spite of clear warnings from the United States. In September 2016, at the G-20 in China, then-President Barack Obama told Russian President Vladimir Putin directly to "cut it out" and that interfering with our election system would cross a line and would have severe consequences.[1] In October, the administration followed up by picking up the famous "red phone" used for nuclear crises to tell their Russian counterparts to not intervene in the 2016 election.[2]

What's also clear is that the Obama administration and U.S. officials thought that these efforts to deter Russia succeeded. The month after the election, President Obama assured the nation in a press conference that "we did not see further tampering of the election process."[3]

But it is now apparent that President Obama was not correct. Russia did not stop its attacks after the Obama administration's warnings. Deterrence failed.

Deterrence failed.

Hack the Vote

In June 2017, *The Intercept* published a highly classified top secret report from the National Security Agency (NSA) that it put together in April, revealing that Russia sought to infiltrate the actual U.S. election system architecture.[4] The NSA report revealed that:

> Russian General Staff Main Intelligence Directorate actors … executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solution … The actors likely used data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations … In October 2016, the actors also created a new email address that was potentially used to offer election-related products and services, presumably to U.S.-based targets.[5]

The Russian plan was fairly straightforward. *The Intercept* explained that Russia sought to "pose as an e-voting vendor and trick local government employees into opening Microsoft Word documents invisibly tainted with potent malware that could give hackers full control over the infected computers."[6]

Russia's hacking campaign began on August 24 with an initial spear-phishing campaign targeting the employees of the electronic voting company. The NSA concluded that, based on Russia's subsequent efforts, "it was likely that at least one account was compromised" at this company.[7] Once the Russians successfully infiltrated the company, they posed as company employees and then sent 122 emails to local government organization email addresses between October 27 and November 1—just two weeks before the election.[8]

The emails that the Russians sent contained a malicious Microsoft Word document that "contained detailed instructions on how to configure EVID software on Microsoft Windows machines."[9] EVID software enables "poll workers to quickly check a voter's registration status, name and address."[10] The NSA determined that "given the content of the malicious email, it was likely that the threat actor was targeting officials involved in the management of voter registration systems."[11] These "Trojanized documents," according to the NSA, likely enabled the Russians to have "persistent access or survey the victim for items of interest."[12] In other words, the Russians could have impacted the actual running of the election.

It has also been revealed that the efforts to hack the election system were more widespread than previously thought. U.S. officials have confirmed that at least 20 states were targets of hackers. There was, therefore, a fairly widespread campaign to infiltrate the U.S. election system.

Some have posited that the Russians were just poking around our election system to learn its vulnerabilities and to map its contours, possibly to intervene in future elections.

But knowing that the Russians did not stop following the Obama administration's warnings, and knowing that they were actively working to help Trump's "election chances" (as the intelligence community assessed in January 2017),[13] and knowing that Russia was seeking to infiltrate the U.S. election system in the months, weeks, and days leading up to the 2016 election, strongly suggests that Russia's 2016 election-hacking efforts were not about future U.S. elections—but were instead in support of their campaign to help Donald Trump.

A question, however, remains: Could a U.S. election even be hacked?

The Department of Homeland Security (DHS) has asserted that the diffuse and decentralized nature of the U.S. electoral system makes it almost impossible to hack. Samuel Liles, the acting director of Cyber Division, Office of Intelligence Analysis in DHS, testified that the intelligence community "looked at diversity of the voting system as a great strength. And the fact that they were not connected in any one kind of centralized way."[14]

However, J. Alex Halderman, a professor of computer science and an election security expert at the University of Michigan, counters this claim in prepared testimony to the Senate Intelligence Community:

> Some say the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make changing a state or national election outcome impossible. Unfortunately, that is not true. Some election functions are actually quite centralized. A small number of election technology vendors and support contractors service the systems used by many local governments. Attackers could target one or a few of these companies and spread malicious code to election equipment that serves millions of voters. Furthermore, in close elections, decentralization can actually work against us. An attacker can probe different areas of the most important "swing states" for vulnerabilities, find the areas that have the weakest protection, and strike there.[15]

So, while the decentralized nature of the U.S. voting system means the Russians could not simply hack into one centralized database in Washington, D.C., the antiquated and outdated technology used in elections was indeed vulnerable. Given that the NSA report was based on material learned this spring, it seems clear that while DHS and the FBI on Election Day may have been looking for signs of a massive cyberattack, a more discrete, targeted effort may not have been noticed.

Put another way, the U.S.' decentralized voting systems may make it somewhat harder to hack, but it also makes any hacking that does occur harder to detect.

Bruce Schneier, a cybersecurity expert at Harvard's Berkman Center, told *The Intercept*, "Hacking an election is hard, not because of technology—that's surprisingly easy—but it's hard to know what's going to be effective … deciding where to hack is really hard to know."[16] Therefore, the theory that the United States is protected by a diffuse and decentralized voting system is not true if cyber actors know where to target or can hit enough targets to make a difference.

In the case of Russia's efforts, it is clear that it does have the resources to do the latter; it could certainly hit enough targets. The question is the former: Would Russia know where to target? While the Russians certainly could have looked at past elections and followed press reports to identify the battleground localities and counties where they should have focused their efforts, it is also the case that their efforts could have been aided greatly if they received data and direction from American campaign experts on where to target. This may therefore become a subject of Robert Mueller's investigation.

Indeed, the FBI has said that it continues to have open investigations into the 2016 election. At the Senate Intelligence Committee hearing, it was revealed by Bill Priestap, assistant director of the Counterintelligence Division of the FBI, that the FBI now has "a number of investigations open" into the hacking of election systems in 2016 that are "all still pending … [W]e continue to learn things" about what happened.[17]

Why Deterrence Failed

While the U.S. is still trying to figure out what happened in 2016 in terms of the election system, what is now clear to U.S. intelligence is that Russia conducted an unprecedented campaign to intervene in the U.S. election. Russia conducted that campaign despite knowing that there would be significant blowback, particularly if Secretary Clinton won, which was widely presumed.

What is now clear to U.S. intelligence is that Russia conducted an unprecedented campaign to intervene in the U.S. election.

Yet Russia not only proceeded with a concerted, multipronged effort to intervene in the U.S. election, but it also did so brazenly. Russia, for instance, hacked the Democratic National Committee during Moscow business hours and left clear digital fingerprints. It also used its overt media channels to echo the messages of the Trump campaign. The intervention was obvious and clear at the time, which is why President Obama warned them to stop.

But Russia proceeded anyway. There are a few reasons for this, some of them unique to the mind-set of the Kremlin.

The first broad reason is that Putin saw a unique opportunity in the 2016 election—and limited downsides to intervening. The Kremlin saw a chance to sow discord in the United States and to back a candidate in Donald Trump who would upend roughly 70 years of Republican foreign policy traditions of being hawkish on Russia. Putin also blamed then-Secretary of State Clinton for fueling protests in Russia in 2011 in reaction to the fraudulent parliamentary elections. He saw an opportunity to disparage her and expected her to adopt a hard-line position toward Russia whether he intervened or not.

Second, the Kremlin sees successful democratic governance as a threat to its own internal control. Cracking down on internal dissidents, suppressing the political opposition, shutting down freedom of press, and closing off political space internally does not actually protect autocrats from democrats. As long as democratic states provide a more attractive model of governance to the citizens of autocratic regimes, the autocrats are vulnerable. In response, Putin set out to undermine democratic governance in the U.S. and Europe in an effort to sully the open democratic model of the West.

Third, Putin actually wants a return to the great power dynamics of the Cold War. He wants to return to the period when Russia was the chief geopolitical adversary of the United States. Once Russia invaded and illegally occupied Crimea and was hit with U.S. and European sanctions in 2014, it concluded that there was no way back to positive relations with the

West and that it would be better for Putin internally to stoke Russian patriotism and then use Russia's vast espionage and cyber tools to sow discord in the West.

It is very hard to deter a country that is seeking a confrontation.

Reestablishing Deterrence

Reestablishing America's ability to prevent future election interference requires a dual strategy that strengthens our ability to deter foreign actors and that strengthens our defenses.

Reestablishing America's ability to prevent future election interference requires a dual strategy that strengthens our ability to deter foreign actors and that strengthens our defenses.

First, the U.S. must strengthen its ability to deter foreign actors. It is imperative that this administration, or Congress, clearly articulate in its messaging that interference in our election process will bring about a series of severe consequences. In a normal administration, a president would give a prominent address laying out the steps that the administration was taking and warning countries of dire consequences for election interference. The president would likely note that we are watching and on guard. And that if we find that countries interfered in our elections, or the democratic elections of our allies, it will be met with a strong response. The response could involve severe economic sanctions, a massive cyber retaliation, or even potentially warning of military action. What is key is that other countries must believe the United States takes this issue deadly seriously and will massively retaliate if its democracy is attacked.

Second, given that an actor like Russia—or even North Korea or Iran—that is already an adversary of the United States may not be easily deterred, it is also essential for the United States to strengthen its defenses. While this involves improving the U.S. election infrastructure, it also involves greatly developing our counterintelligence and cyber capabilities to improve our ability to detect and respond to foreign hacking efforts. An independent commission, modeled on the 9-11 Commission, is needed to identify gaps and to put forth recommendations for how to fill those gaps.

The United States cannot allow regular foreign intervention to become a reality. It must now treat efforts to influence or infiltrate our elections as a top-tier national security threat, and it must take action to deter and defend against efforts to intervene in American democracy. Time is wasting, action is needed, and it is needed right now.

[1] Massimo Calabresi, *Inside the Secret Plan to Stop Vladimir Putin's U.S. Election Plot*, Time (July 20, 2017), http://time.com/4865982/secret-plan-stop-vladimir-putin-election-plot/.

[2] Michael Riley & Jordan Robertson, *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, Bloomberg (June 13, 2017), https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[3] Matthew Cole et al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (June 5, 2017), https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

4. *Id.*

5. *Report on Russia Spearphishing*, National Security Agency 1, https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1.

6. Cole et al., *supra* note 3.

7. *Report on Russia Spearphishing*, *supra* note 5, at 3.

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.* at 3-4.

13. *Assessing Russian Activities and Intentions in Recent US Elections*, Office of the Director of National Intelligence (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

14. *U.S. Senate Select Committee on Intelligence Hearing*, U.S. Senate Select Committee on Intelligence (June 21, 2017), https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections.

15. J. Alex Halderman, *Expert Testimony by J. Alex Halderman, Professor of Computer Science, University of Michigan*, U.S. Senate Select Committee on Intelligence 3 (June 21, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf.

16. Cole et al., *supra* note 3.

17. *U.S. Senate Select Committee on Intelligence Hearing*, *supra* note 14.

RECOMMENDATIONS

So, where do we go from here?

Many of the problems described above have clear, attainable solutions. Others present more vexing challenges, and require further research and analysis to identify the best solutions.

The FEC and internet platform companies should require political advertisers to say who they are.

First, requiring disclaimers stating who paid for digital political ads *should* be an easy fix for the FEC. Federal statutes already dictate that such disclaimers are required, and technology has changed enough in recent years that the FEC's earlier reasons for exempting digital ads are no longer applicable. In late 2017, in response to an advisory opinion request CLC filed on behalf of Take Back Action Fund, the FEC stated, for the first time, that full disclaimers are required on certain Facebook political ads. The FEC is also expected in early 2018 to open a rulemaking to clarify the rules on all digital ad disclaimers.

Large tech companies like Facebook and Twitter have also pledged to give viewers more information about who is paying for an ad,[1] although many questions remain about how those new policies will be carried out.

Yet there are limits to how much the FEC can accomplish, and to what we can expect internet platforms to voluntarily do on their own. For example, the FEC cannot require disclaimers or disclosure for digital ads that don't expressly advocate for or against a candidate, since online ads are not covered under current statutes regulating "electioneering communications." And companies like Facebook and Google have talked about self-regulation, but what is in their self-interest does not always align with the public interest. More robust reform will have to come from Congress.

Congress should strengthen disclosure laws, including by passing the bipartisan HONEST Ads Act.

Legislative solutions like those included in the bipartisan HONEST Ads Act (described above) would be a good first step toward shoring up the vulnerabilities exploited by Russia in 2016. The bill would require both disclaimers and reporting for digital ads that mention a candidate and air near an election—just like television or newspaper ads. Moreover, it would create greater transparency around the content of the ads themselves.

The HONEST Ads Act would create some parity between digital and broadcast ads. However, it would not fix the underlying transparency problems that allow dark money groups to buy ads on any platform while keeping donors—including any foreign donors—a secret. Routing $2 million through dark money vehicles is how Great America PAC officials offered to help a fictitious Chinese donor funnel money into U.S. elections without detection, for example.

The latest version of Senator Sheldon Whitehouse's DISCLOSE Act would help close the disclosure loopholes that could allow foreign governments and individuals to secretly launder money into U.S. elections. That bill would require public disclosure of all major donors to groups spending money in elections.[2]

Moreover, the 2017 version of DISCLOSE would limit the ability of foreign-owned corporations—like the Chinese-owned corporation that *The Intercept* revealed had contributed to Jeb Bush's super PAC—to spend money in U.S. elections.[3] Alaska is considering a similar ballot measure that would establish similar thresholds to prohibit any "foreign-influenced corporation" from making contributions.[4]

Congress should hold hearings and gather information to carefully craft laws that address the regulation of foreign money used for genuinely issue-based social media activity.

A more challenging question is how to address foreign influence efforts that do not involve obvious partisan political messages or that may not involve obvious transfers of money.

Some of Russia's digital communications—paid ads and otherwise—might not fall under the existing foreign national ban because the messages discussed divisive political or social issues rather than candidates or elections. This may suggest that part of Russia's goal was to widen existing divides by inflaming political passions around issues like the Black Lives Matter movement or the Second Amendment. There are no current legislative proposals that would limit foreign nationals from conducting such activities—although the HONEST Ads Act would require that platforms make the content of such ads publicly available—and a broader question is whether a foreign national's digital communications about political issues that don't implicate candidates or elections *should* be limited. As Facebook has noted, "Organizations such as UNICEF, Oxfam or religious organizations depend on the ability to communicate—and advertise—their views in a wide range of countries."[5] It is a challenge to craft policies that would limit a foreign country's ability to influence elections by targeting divisive social messages without also affecting other forms of international communications.

At the very least, however, Congress should conduct a careful and balanced inquiry into the relevant issues, including where disclosure laws, as opposed to more restrictive measures, would be most effective to bridge various concerns.

Further research and analysis are needed to develop an effective approach to social media bot activity.

The 2016 elections also showed how our existing campaign finance framework is not equipped to address Russia (or any other foreign country) creating thousands of fake social media accounts and using automated "bots" to help messages go viral and reach wider audiences. We know how to regulate foreign nationals spending money on digital political ads, but it is less clear how to address bots disseminating messages without ever making payments to the platform hosting those messages.

Traditionally, bot policy has been a self-regulatory matter for social media companies. Given the growing awareness of how bot usage can have political ramifications, it is clear that this is not enough. We must carefully assess which elements of bot policy should be within the control of government and which should be left to self-regulation.

As Guilbeault and Gorwa note, the challenge for policymakers and social media companies is how to prevent the use of bots for political manipulation and astroturfing, without hampering automation's pro-democracy uses. Some of the demonstrated problems with social media self-regulation can be remedied by companies being more transparent about their bot reviews and providing greater access to data for unbiased third-party researchers, as well as creating mechanisms for users to engage in the process.

More research is certainly needed on how political actors are spending money on bots, both within the U.S. and abroad, by firms such as Cambridge Analytica and Deeproot that use machine learning and data analytics in political campaigns, both in the U.S. and abroad.

The public and private sectors should strengthen voters' media literacy.

Even if new online transparency policies are implemented—and especially if they are not—it will be important to improve voters' media literacy in the midst of an increasingly complex online political landscape. Ensuring that voters have the tools to read online content critically and evaluate sources of information is a necessary safeguard against foreign attempts to circulate fabricated or misleading content.

This is particularly important as the share of the public getting at least some of their news from social media platforms like Facebook continues to increase—in Gallup's measure, the share rose to 67 percent in 2017.[6] However, many people struggle with evaluating content posted on social media. A group of Stanford researchers, for example, found that a number of students had difficulty distinguishing real news from fake news on social media, including understanding what Facebook's "sponsored content" designation meant.[7]

Some organizations are tackling this issue head on. Groups like the News Literacy Project[8] and the National Association for Media Literacy Education,[9] for example, have been working on teaching students and adults how to be critical news consumers for years. Research also indicates that people who know more about the workings of the news media were less likely to believe conspiracy theories.[10] And the recently announced News Integrity Initiative hopes to combat fake news through a variety of means, including raising public awareness on news literacy issues, promoting excellent journalism, and bringing news literacy instruction to high school classrooms. This initiative has attracted Facebook as a major donor.[11]

Congress should bolster our election infrastructure security and modernize voting equipment.

Moving from influencing votes to casting votes, any effort to guard against future foreign meddling requires protecting our election infrastructure. This includes bolstering security, modernizing voting equipment, preparing election officials for the newest threats, and continually testing and improving election systems across the country.

In the past, Congress had shown a willingness to address the vulnerabilities of election infrastructure. In particular, in the wake of the 2000 elections, Congress passed the Help America Vote Act (HAVA). Among other reforms, HAVA created the Election Assistance Commission and made $4 billion available for states to improve their election systems.[12] Fifteen years later, however, many states are in need of substantial reinvestments.

Steps that could be taken include replacing outdated voting machines, improving coordination and communication between states and the federal government, ensuring every vote has a paper trail, regularly checking voting machines, and performing full-fledged audits after every election.[13]

Bipartisan legislation is pending in both chambers of Congress that would start to address some of these gaps, including by making states aware of vulnerabilities, providing them resources to increase their systems' security by allowing them to apply for federal grants, and working to agree on best practices.[14] Another bipartisan bill would fast-track security clearances for certain high-level election officials; this would allow them access to classified information on hacking threats.[15] For its part, the Senate Intelligence Committee is expected to issue recommendations of its own when it releases its report on Russia's hacking attempts.[16]

Additionally, in December 2017, a bipartisan group of senators introduced the Secure Elections Act, which would take a number of important steps toward modernizing our election infrastructure and protecting against cyberattacks. If passed, the bill would establish new election security guidelines, give states block grants for upgrading their voting equipment and systems, facilitate information sharing about threats from the federal down to the local level, give state election officials security clearances, and institute other sorely needed protections.[17]

The White House has not taken any steps to address these issues. In fact, the Presidential Advisory Commission on Election Integrity (commonly referred to as the Pence-Kobach Commission) could have actually increased security risks with its plan to build a national voter database with millions of voters' personally identifying information.[18]

As nine former national security and technology officials, including former Director of National Intelligence James Clapper, warned in an amicus brief filed in a D.C. District Court case regarding the Commission, a national database "may be a compelling target for foreign adversaries seeking to interfere in future elections through a variety of means, as well as for cyber criminals and other malicious actors."[19]

Addressing foreign interference must be treated as a national priority.

Finally, the U.S. must treat foreign meddling in our elections as a top-tier national security threat, and take decisive action to deter and defend against efforts to intervene in American democracy.

There is every reason to believe that the experience of 2016 will be repeated in elections to come. The desire for foreign actors to influence or disrupt U.S. elections is not going away.

The question now is what we are going to do to stop them.

[1] *See* Rob Goldman, *Update on Our Advertising Transparency and Authenticity Efforts*, Facebook Newsroom (Oct. 27, 2017), https://newsroom.fb.com/news/2017/10/update-on-our-advertising-transparency-and-authenticity-efforts/. *See also* Bruce Falck, *New Transparency for Ads On Twitter*, Twitter Blog (Oct. 24, 2017), https://blog.twitter.com/official/en_us/topics/product/2017/New-Transparency-For-Ads-on-Twitter.html.

[2] Democracy Is Strengthened by Casting Light On Spending in Elections Act, S. 1585, 115th Cong. (2017).

[3] *Id*. Another bill, the Get Foreign Money Out of U.S. Elections Act, would similarly change the definition of foreign-influenced corporation. *See* Get Foreign Money Out of U.S. Elections Act, H.R. 1615, 115th Cong. (2017).

[4] *The Alaska Government Accountability Act: A Bill By Initiative* 3-4, http://www.elections.alaska.gov/petitions/17AKGA/Bill.pdf.

[5] Elliot Schrage, VP of Policy and Communications, *Hard Questions: Russian Ads Delivered to Congress*, Facebook Newsroom (Oct. 2, 2017), https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/.

[6] Elisa Shearer & Jeffrey Gottfried, *News Use Across Social Media Platforms 2017*, Pew Research Center (Sept. 7, 2017), http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

[7] Brooke Donald, *Stanford researchers find students have trouble judging the credibility of information online*, Stanford Graduate School of Education (Nov. 22, 2016), https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online.

[8] *Program*, The News Literacy Project, http://www.thenewsliteracyproject.org/about/program (last visited Dec. 21, 2017).

[9] *About*, National Association for Media Literacy Education, https://namle.net/about/ (last visited Dec. 21, 2017).

[10] Craig Chamberlain, *Conspiracy thinking less likely with greater news media literacy, study suggests*, Illinois News Bureau (Nov. 29, 2016), https://news.illinois.edu/view/6367/584207.

[11] Emily Dreyfuss, *Facebook pushes news literacy to combat a crisis of trust*, Wired (Apr. 6, 2017), https://www.wired.com/2017/04/facebook-pushes-news-literacy-combat-crisis-trust/.

[12] Cory Bennett, Eric Geller, Martin Matishak, & Tim Starks, *Cash-strapped states brace for Russian hacking fight*, Politico (Sept. 3, 2017), https://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266.

[13] *See* Danielle Root & Liz Kennedy, *9 Solutions to Secure America's Elections*, Center for American Progress (Aug. 16, 2017), https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/. *See also* Lawrence Norden & Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice 6 (2017), https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf.

[14] Michael Sozan, *On HAVA's 15th Anniversary, Congress Needs to Make U.S. Elections More Secure*, Center for American Progress (Oct. 26, 2017), https://www.americanprogress.org/issues/democracy/reports/2017/10/26/441417/on-havas-15th-anniversary-congress-needs-to-make-u-s-elections-more-secure/.

[15] Martin Matishak, *The time to hack-proof the 2018 election is expiring—and Congress is way behind*, Politico (Nov. 26, 2017), https://www.politico.com/story/2017/11/26/election-cybersecurity-hackers-midterms-259472.

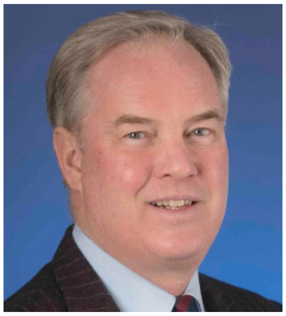
[16] *Id*.

[17] Secure Elections Act, 115th Cong. (2017).

[18] *See, e.g.,* Letter from Kris Kobach to Secretary Denise Merrill (June 28, 2017), https://www.washingtonpost.com/blogs/wonkblog/files/2017/06/PEIC-Letter-to-Connecticut-1.pdf.

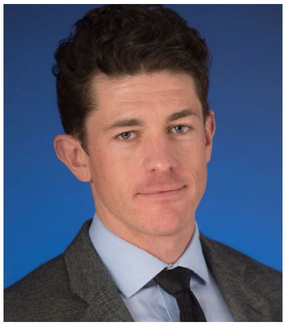
[19] Brief of Former National Security and Technology Officials as Amici Curiae Supporting Plaintiffs' Memorandum in Opposition to Defendants' Motion to Dismiss at 2, Common Cause et al. v. Presidential Advisory Commission on Election Integrity et al., No. 1:17-cv-01398-RCL (D.D.C. Dec. 5, 2017), http://www.law.georgetown.edu/academics/centers-institutes/constitutional-advocacy-protection/upload/common-cause-amicus-brief.pdf. The brief also noted that "aggregating large volumes of personal data in one centralized location" poses a significant risk for foreign attacks and further that "[t]he Commission has compounded these risks by hosting the database on a White House system that has never been used to store information of this kind and may lack core safeguards." *Id.* at 3.

ABOUT THE AUTHORS



Trevor Potter is the founder and president of Campaign Legal Center, a former chairman of the Federal Election Commission, and a senior adviser to the reform group Issue One. He also heads the political law practice at the Washington firm of Caplin & Drysdale. To many, he is perhaps best known for his recurring appearances on "The Colbert Report" as the lawyer for Stephen Colbert's super PAC, Americans for a Better Tomorrow, Tomorrow, during the 2012 election.

The American Bar Association Journal has described Potter as "hands-down one of the top lawyers in the country on the delicate intersection of politics, law and money." A Republican, he was appointed to the FEC in 1991 by President George H.W. Bush, and then served as general counsel to John McCain's 2000 and 2008 presidential campaigns. He was a member of the legal team that successfully defended the McCain-Feingold reform law in the Supreme Court, prior to the *Citizens United* decision. A nonresident senior fellow in Governance Studies at the Brookings Institution, Potter is the author of several books and manuals on lobbying regulation and disclosure, campaign finance, and federal election law. He has testified before Congress on federal election proposals and campaign finance regulation, and has taught campaign finance law at the University of Virginia School of Law and Oxford University. He has served as chair of several American Bar Association election law and lobbying regulation committees and task forces, and is currently a member of the ABA's Standing Committee on Election Law as well as the American Law Institute.



Brendan Fischer joined CLC in March 2016 and now directs CLC's work before federal regulatory agencies, such as the Federal Election Commission (FEC), to ensure vigorous and fair enforcement of campaign finance and ethics laws, and to hold candidates and political committees accountable for violating those laws.

Fischer has expertise in campaign finance, government ethics, lobbying, and political transparency issues, and is a frequent commentator for national news publications, including *The Washington Post*, *Los Angeles Times*, *USA Today*, *POLITICO*, *Time*, *Slate*, *Wired*, *The Daily Beast*, *The Intercept*, CNN, and NBC News. He also has spoken at conferences and events nationwide on money-in-politics issues. Fischer was previously general counsel with the Center for Media and Democracy, where he led the watchdog group's legal research and advocacy efforts.

Douglas R. Guilbeault is a researcher in the Network Dynamics Group and a Ph.D. student at the Annenberg School for Communication at the University of Pennsylvania. Guilbeault is also an affiliated researcher of the ComProp project at the Oxford Internet Institute and the Digital Intelligence Lab at the Institute for the Future. Guilbeault is a computational social scientist who studies social bots and conducts online experiments to study collective dynamics. His writing on bots has appeared in the *International Journal of Communication*, *The Atlantic*, *Wired*, and *Quartz*. He is the author, along with Samuel Woolley, of the report, *Computational Propaganda in the United States of America:* Manufacturing Consensus Online.

Robert Gorwa is a doctoral student in the University of Oxford's Department of Politics and International Relations and a researcher affiliated with the ComProp project at the Oxford Internet Institute. Gorwa's research on bots focuses on the theoretical and policy-oriented ramifications of social media manipulation. He is interested in the various methodological approaches to studying bots, the history and theory of propaganda, and the contemporary technology policy and regulatory issues around content, automation, and moderation. His writing on these topics, along with writing on technology and politics more generally, has been featured in Foreign Affairs, The Washington Post, Wired, Quartz, and other outlets.

Daniel A. Petalas is an owner in the Washington, D.C., office of Garvey Schubert Barer and focuses his practice on white collar and government investigations. As the former acting general counsel and head of the Enforcement Division of the Federal Election Commission, Petalas supervised the Commission's litigation, enforcement, and investigative programs.

For nine years prior to his work on the FEC, Petalas was a federal corruption prosecutor at the U.S. Department of Justice in its Public Integrity Section. There, he worked closely with the FBI and numerous Offices of Inspectors General to investigate the full array of financial and corruption offenses, including fraud, theft, money laundering, embezzlement, bribery, false statements, and obstruction of justice. Petalas was a member of the team that investigated and prosecuted the Jack Abramoff-related lobbying scandal, resulting in 21 guilty pleas and convictions, and helped supervise the FBI investigation of a former federal judge, who ultimately was impeached based on evidence obtained during the investigation. Before his federal government service, Petalas was a litigation associate in the Dallas and Washington, D.C., offices of Vinson & Elkins, LLP and clerked for Judge Thomas M. Reavley on the U.S. Court of Appeals for the Fifth Circuit.

Max Bergmann is a senior fellow at the Center for American Progress, where he focuses on European security and U.S.-Russia policy. From 2011 to 2017, he served in the U.S. Department of State in a number of different positions, including as a member of the secretary of state's Policy Planning Staff, where he focused on political-military affairs and nonproliferation; special assistant to the under secretary for arms control and international security; speechwriter to Secretary of State John Kerry; and senior adviser to the assistant secretary of state for political-military affairs. Prior to serving in the State Department, Bergmann worked at the Center for American Progress as a military and nonproliferation policy analyst and at the National Security Network as the deputy policy director.

ABOUT CAMPAIGN LEGAL CENTER

Campaign Legal Center (CLC) is a nonpartisan, nonprofit organization based in Washington, D.C. Through litigation, policy analysis, and public education, CLC works to protect and strengthen the U.S. democratic process across all levels of government. CLC is adamantly nonpartisan, holding candidates and government officials accountable regardless of political affiliation.

CLC was founded in 2002 and is a recipient of the prestigious MacArthur Award for Creative and Effective Institutions. Its work today is more critical than ever as it fights the current threats to our democracy in the areas of campaign finance, voting rights, redistricting, and ethics. Most recently, CLC argued *Gill v. Whitford*, the groundbreaking Supreme Court case seeking to end extreme partisan gerrymandering. In addition, CLC plays a leading watchdog role on ethics issues, providing expert analysis and helping journalists uncover ethical violations, and participates in legal proceedings across the country to defend the right to vote.

CLC

ADVANCING DEMOCRACY THROUGH LAW

15 YEARS