TRUTH ON THE BALLOT

Fraudulent News, the Midterm Elections, and Prospects for 2020

PEN AMERICA

The Freedom to Write

pen.org

Truth on the Ballot: Fraudulent News, the Midterm Elections, and Prospects for 2020

Executive Summary

In this report, PEN America examines the steps taken by technology companies, government actors, and political parties to curb the influence of fraudulent news in the 2018 U.S. midterm elections; examines current legislative proposals to regulate political advertising transparency online; parses the role fraudulent news played in the midterm election cycle; and concludes with recommendations to stakeholders on steps to combat fraudulent news while protecting free expression rights ahead of the 2020 elections.

This report builds on PEN America's October 2017 report, *Faking News: Fraudulent News and the Fight for Truth*, which examined how fraudulent news is eroding truth-based civic discourse and constitutes a threat to free expression. Then, as now, PEN America defines fraudulent news as *demonstrably false information that is being presented as a factual news report with the intention to deceive the public.* This report focuses on examples that meet this definition and other forms of disinformation that are presented as truth with the intent to deceive.

For the average American, the 2016 election cycle represented the frightening debut of fraudulent news as a malicious contribution to our national politics. Today, our society is still struggling with the implications and consequences of Russia's 2016 disinformation campaign, as well as the efforts of disinformation actors motivated by profit or ideology. **Today, the danger is that fraudulent news and disinformation will become normalized as unsavory but acceptable campaign tactics—just another part of the toolbox of hotly contested modern campaigns.** Given this risk, the threat that fraudulent news poses—not only to our political processes, but to our shared foundation of objective truth—has only grown since 2016, and must be taken seriously as the 2020 election cycle begins.

Key Conclusions

- Russian disinformation continues to be a salient threat to our elections, and **Russian agents of disinformation are playing a 'long game'**: their focus is not merely on influencing American electoral processes, but on stoking political polarization and sowing distrust in democracy.
- In the past two years, experts and observers have noted a worrying **increase in instances of domestic disinformation**, with American political actors utilizing fraudulent news and disinformation against political opponents.
- Today, perhaps the greatest threat that fraudulent news poses is the risk that it will become a normalized part of U.S. political discourse. **There is a real danger that fraudulent news may become the new normal: a distasteful, but not disqualifying political tactic**.
- Technology companies have made significant efforts to reduce the spread of fraudulent news, the results of which are mixed: **while important advances have been made, many efforts remain insufficient, while others have caused new problems**. Voluntary efforts by technology companies to ensure transparency regarding advertisements on their platforms have so far proven insufficient to prevent their manipulation.
- **Micro-targeting capabilities on the platforms have weaponized disinformation**, so that what might once have passed muster as simply a hard-edged campaign message in the public arena can now move with stealthy, laser-like efficiency to reach sub-segments of voters while remaining invisible to the wider public or opposing campaigns.
- **While both human and automated content review are subject to bias, some combination of the two is likely the most reasonable approach.** It is imperative that the platforms that host such a vast

portion of our political discourse supplement their current tools with greater numbers of qualified, trained, and sufficiently supported personnel to evaluate content, exercise judgment, and adapt to fast-changing threats.

- Fraudulent news and disinformation in the 2018 midterm election cycle tended to have one of a few objectives: **attacking individual candidates, dampening turnout or stoking distrust in the voting process, or amplifying a desired narrative about a particular political event.** Key examples of the latter included disinformation regarding the confirmation hearing of Supreme Court Justice Brett M. Kavanaugh and the contingent of Central American migrants that moved towards the U.S. in the fall of 2018.
- During elections, individual **candidates, political parties, and party committees have a critical and fundamental role in protecting the integrity of our civic discourse** and the public's ability to make informed decisions about who will represent them.
- **Empowered consumers of information are society's best defense against the scourge of fraudulent news** and attempts to undermine the role of truth in our society. Efforts to equip citizens to distinguish truth from falsehoods and make informed political decisions are therefore critical to curbing the impact of fraudulent news.

Efforts to Combat Fraudulent News

Since the fallout from the 2016 elections, technology companies have taken a series of steps designed to blunt the impact of fraudulent news. PEN America's report examines the actions of three major platforms: Facebook (which additionally owns Instagram), Twitter, and Google (of which YouTube is a subsidiary). All the platforms face the seemingly contradictory pressures of removing fraudulent information while also protecting free expression and avoiding the role of unaccountable global censor.

Platforms have generally responded with actions including: revisions to their algorithms; partnerships with third-party fact-checkers and other civic initiatives; increased transparency regarding their advertisements and advertising policies; new waves of account shutdowns for non-compliance with Terms and Conditions; and more active collaboration with political campaigns and the government to proactively combat fraudulent news. The question of whether these new efforts have been successful in stemming the tide of fraudulent news remains unanswered. While several studies have encouragingly indicated that these new tactics have had some success, others argue any self-congratulation is premature.

One key question involves when and how Facebook, Twitter, or Google chooses to shut down the account of a user disseminating fraudulent news or exhibiting behavior indicating the account is 'inauthentic'. Account shutdowns are widely seen as the most effective and direct way to stop purveyors of fraudulent information, but as a tactic they also represent the most significant risk to the free speech of a platform's users. Given these dueling concerns, companies must exercise a remarkable amount of care and consistency in both the formulation and the application of their criteria for shutting down accounts, and must ensure appeal mechanisms are clear and accessible.

Additionally, tech company collaboration with government actors offers a proactive means for addressing fraudulent news, but also carries risks to user privacy and free expression. At a minimum, increased transparency around these initiatives is imperative, and social media platforms must be as open as they can with users about what type of information they might share with government bodies and how they decide what to share and when.

PEN America's report examines the issue of ad transparency in depth. Google, Twitter, and Facebook all sell political ads, and in 2016 foreign agents used these platforms' ad services to spread disinformation, sow dissension, and suppress voter turnout. In response, all three companies have

created their own searchable ad databases, a major effort at increasing the transparency of advertising on their platforms. Even so, critics argue that this is no substitute for legislative solutions like the Honest Ads Act or the For the People Act. While PEN America views legislative solutions to fraudulent news with caution, there are several elements of such proposals that PEN America believes represent positive steps forward. In particular, increased transparency regarding who funds political ads is a vital step towards enabling users to make informed decisions.

Currently, there are a collection of examples where platforms have failed to adequately enforce their existing ad transparency rules, suggesting that current transparency efforts remain insufficient. At the same time, there is the danger of overly aggressive action that would risk conflating political ads with other ads of public importance. This was—and remains—a concern for Facebook's policies regarding "issue ads," which risks lumping journalism and community engagement efforts into the same category as political advertising.

Fraudulent News in the 2018 Election Cycle

Fraudulent news and information—from both foreign and domestic sources—remained on full display during the 2018 midterm elections cycle. Some of the most significant examples included attacks on specific candidates for public office, disinformation aimed to suppress voter turnout and undermine confidence in the election process, and fraudulent information related to significant political debates—for example regarding the movement of Central American migrants towards the U.S. in the fall of 2018, or the testimony of Christine Blasey Ford during the confirmation hearings for Supreme Court Justice Brett Kavanaugh.

As more is revealed about the ongoing threat from Russian disinformation campaigns, it becomes clear that in addition to attempts in 2016 to spread disinformation with a specific electoral outcome in mind, there are ongoing efforts to stoke existing divisions in American society and undermine trust in democratic institutions, without necessarily attempting to advance any particular ideology or candidate. Russian disinformation campaigns, the existing evidence suggests, are playing a long game, stoking division and pushing more extreme political rhetoric with an eye toward weakening national cohesion and our democracy.

In addition to ongoing efforts originating overseas, numerous experts have concluded that much of the fraudulent news in the midterm election cycle came from domestic actors on both the left and the right. The increasing prevalence of an ends-justify-the-means mentality towards the use of fraudulent news and disinformation raises the danger that these tactics may become part of the toolbox of hotly contested campaigns: distasteful, but not disqualifying. It is this normalization of fraudulent news that poses perhaps the greatest threat to our civic discourse.

Conclusions and Recommendations

PEN America ends our report with a series of conclusions and recommendations to technology companies, political groups, the government, and others. Consistent with our conclusions in *Faking News*, PEN America continues to advocate for solutions that empower everyday citizens—as consumers of online information—to critically evaluate the factual content of the news and information they consume. News literacy is not only society's best defense against the scourge of fraudulent news, but it is also the most effective way to maintain a shared, truth-based foundation of civic discourse while upholding our cherished commitment to protecting freedom of expression within the public square. Ultimately, the most effective, proactive tactic against fraudulent news is a citizenry that is well-equipped to detect and reject fraudulent claims.

At the same time, more urgent action is also needed. Amongst our recommendations, we urge legislators to establish a federal commission to research and analyze ways to combat the spread of

disinformation. We call upon social media platforms to establish and sufficiently support substantial teams of lawyers, advertising experts, linguists, graphics experts and election experts to augment still-developing and experimental artificial intelligence and algorithmic approaches and bring a trained, expert human eye to content in the lead-up to the 2020 elections. We close by calling on politicians, aspirants for public office, and political parties to pledge not to tolerate fraudulent news as a tactic in political debate, even when such fraudulent stories may benefit them politically. To that end, we have created the PEN America Model Pledge Against Fraudulent News. It is our hope that this model pledge can stimulate public support for such a commitment from our nation's highest public servants.

INTRODUCTION

Widespread recognition of the powerful role of fraudulent news and disinformation during the 2016 presidential election put political parties, candidates, social media platforms, oversight bodies and the public on notice that American democracy is vulnerable to a new danger. While we will never know whether the influence of malign actors had a decisive role in the outcome of the vote, the fact that aggressive, broad and stealthy campaigns were waged with the aim of influencing the outcome of the ballot is enough to substantiate that our democratic systems face a serious threat. While the prevalence and impact of fraudulent news came as a surprise to many in 2016, all stakeholders are now on notice concerning the motives and methods of those who use subversive digital information strategies with the aim of exerting improper influence on voters. Tracking and monitoring manifestations of fraudulent news, assessing the efficacy of attempts to combat it, and advancing sophistication and comprehensiveness of such strategies has become a matter of paramount importance to the health of the American body politic. PEN America has undertaken an examination of the state-of-play for fraudulent news in the context of the 2018 midterm elections in order to help inform and drive forward these efforts and set the stage to more effectively combat fraudulent news when Americans next go to the polls en masse in 2020.

In the months and years since 2016, the American public definitively learned, after significant research and consternation, that Russian operatives strategically stoked political divisions and spread disinformation in the United States via social media;[1] that those efforts were intended to influence the 2016 election and were sanctioned by the Russian government; and that at least some of them intentionally tried to sway the race in Donald Trump's favor.[2] These findings were reinforced in December 2018, when two third-party reports produced for the Senate Intelligence Committee detailed the sweeping extent of Russian involvement in the presidential campaign to support Donald Trump's candidacy; turn voters against Hillary Clinton; heighten distrust in U.S. institutions, particularly elections; and divide Americans by race, religion, and ideology.[3]

The Internet Research Agency (IRA), the Russian troll factory behind the online disinformation campaign, reached 126 million people on Facebook, at least 20 million on Instagram (owned by Facebook), and 1.4 million on Twitter and uploaded upward of 1,000 videos to YouTube (owned by Google), according to one of the Senate reports.[4]

The U.S. government and technology platforms were slow in acknowledging the role of foreign interference in 2016. In contrast, the 2018 midterm general elections, in which hundreds of candidates competed for 35 Senate seats and 435 House seats across the United States, were marked by a heightened awareness of the potential for fraudulent news to wreak havoc. "There is more interest both from people and citizens, as well as from parties and elected officials, in understanding how the technological world is shifting," said Tara McGowan, CEO of Acronym, a progressive digital strategy organization, who worked on President Obama's 2012 digital campaign team.[5] As the problem of fraudulent news online has become more widely acknowledged, tech companies and others have experimented with an array of possible solutions. Among them were some that showed promise, some that were ineffective, and some that swept up and suppressed legitimate information. Reliance on algorithms and artificial intelligence to render subtle judgements on matters of politics, race, history, and language sometimes led to nonsensical or perverse outcomes that could have been avoided through more intensive involvement of trained staff. The preparation for the 2018 midterm elections also demonstrated the risks of social media platforms under pressure to act but not fully equipped to do so in ways that are sufficiently calibrated and informed to respect and protect free expression.

It would be too sweeping and simplistic to say that 2018 was "better" than 2016. For one, the impact of 2016 is still being revealed. "The fake news apocalypse we feared for the midterms already happened—back in 2016," Charlie Warzel of Buzzfeed noted.[6] "We're now living in its aftermath. And the misinformation, propaganda, and hyper-partisan news that has defined this election news cycle reveals an unsettling truth: that years of algorithmically powered information warfare have drastically rewired our political discourse, turning it ever more toxic and blurring the lines of reality."[7]

As Nina Jankowicz, a global fellow at the Wilson Center's Kennan Institute, told PEN America: "I think it's easy to conclude that things went better than 2016. But I'm not so sure. Facebook is still playing whack-a-troll and left up over 100 [Russian-run] Internet Research Agency accounts until the last second and only identified them because they got tipped off by the FBI."[8] What was different this election cycle, she said, was the presence of more discernible disinformation from "homegrown actors": Americans who were spreading false stories for political purposes. This included false allegations of voter fraud and vote rigging, some of them made on Election Day itself.[9] These measures, adopted by campaigns, political organizations and rogue individual actors, point to a gradual degradation of the standards and reliability of our political discourse, perhaps sparked by outside actors but compounded by the sense that any campaign not using state-of-the-art information warfare weapons would be outmatched.

At the same time, the nature of the threat has evolved. "Yes, misinformation was a problem in the 2018 midterms, but it wasn't the 100 percent fabricated articles that we saw in 2016," Claire Wardle, an expert in disinformation and executive director of First Draft News, told PEN America.[10] "The most influential driver of disinformation was stand-alone visual posts and memes. They took advantage of the deep partisan divisions, and much of the content was designed to reinforce positions and denigrate the other side, using dog whistles, logical fallacies, and false equivalency."[11]

Despite the heightened awareness and new procedures and strategies put in place for 2018, it is impossible to conclude that the information ecosystem is better defended in 2018 than in 2016, particularly given the opaque and evolving nature of the threat. Researchers on the effectiveness of technology companies' tactics against fraudulent news have hesitated to draw any categorical conclusions as to whether the fight is being won. Meanwhile, purveyors of fraudulent news have been changing their tactics, accelerating an arms race between those attempting to block fraudulent news and those attempting to promote it. The 2018 election cycle still bore witness to a collection of fraudulent news stories—including allegations against specific candidates and fear-mongering stories about political events. Perhaps most worryingly, a growing group of domestic political actors have shown a willingness to see fraudulent news as an unsavory but acceptable political tactic to employ against their opponents, defending their actions through an end-justifies-the-means mentality. In short, fraudulent news remains a salient threat to our politics. Political parties, campaigns, regulators and technology companies are on notice that the integrity of the 2020 US election will depend upon their ability to mount more effective defenses than exist today.

OVERVIEW

This report focuses on the role of fraudulent news in the 2018 U.S. midterm general elections. It examines initiatives undertaken by tech companies, the government, advocacy organizations, campaigns, and political parties to anticipate and counter the spread of fraudulent news and disinformation during the elections and analyzes the possible benefits and risks of these efforts, particularly from the perspective of how they might protect or infringe upon freedom of expression. The report also provides an overview of patterns and specific instances of fraudulent news that occurred during the election period and ends with conclusions and recommendations for 2020.

In 2017, PEN America published *Faking News: Fraudulent News and the Fight for Truth*, which warned of the threat that fraudulent news poses to free expression, as well as the risk that efforts to counter it could also abridge those rights.[12] That report evaluated the array of strategies that Facebook, Google, Twitter, newsrooms, and civil society groups were employing to address the problem and suggested solutions that focused on empowering news consumers while vigilantly avoiding new infringements on free speech.

PEN America defines fraudulent news as **demonstrably false information that is being presented as a factual news report with the intention to deceive the public.** In this study, the term does not refer to good-faith mistakes, biased news reports, or editorial decisions to focus more on one particular issue than another. In the context of President Trump's ongoing rhetorical attacks on the media and his predilection for describing any unfavorable coverage as "fake news," these distinctions take on ever greater importance. The intended effect of Trump's rhetorical campaign, which has been worryingly successful, is to leave many in the public confused and uncertain about what to believe.[13]

In this report, we will focus on examples that meet the above definition of fraudulent news and will look at other forms of disinformation that, while perhaps not presented as a factual news report, are nonetheless presented as truth with the intent to deceive. Cybersecurity issues that

fall outside this category, such as phishing attacks and hacking, are not within the purview of this paper.

The 2018 midterm elections were held on November 6, with 35 of the 100 Senate seats and all 435 seats in the House of Representatives contested. Another 36 states and 3 territories held gubernatorial elections. Voter turnout, at 49.3 percent of eligible voters, was the highest for a midterm election since 1914.[14] Republicans maintained control of the Senate, gaining two seats, while Democrats took back control of the House, gaining 41 seats.

This report focuses on the 2018 midterm elections and on actions by technology companies and other stakeholders to address fraudulent news in advance. Most of those actions occurred in 2018, but where relevant the report will touch on events from 2017, including the Alabama special elections.

As new revelations about disinformation in the 2016 elections continue to come to light more than two years later, we recognize that we do not currently know everything that has happened during the 2018 midterm elections. With the 2020 campaign already starting, however, now is the time to consider the lessons learned. While elections heighten both the threats and the stakes for fraudulent news, it is not an election-specific problem but a continual one that the U.S. government, citizens, and tech companies will be grappling with for the foreseeable future.

Why Fraudulent News is a Free Expression Issue

At the 1948 PEN Congress in Copenhagen, PEN America joined its sister PEN centers around the world in adopting the PEN International Charter, which states in part that "since freedom implies voluntary restraint, members pledge themselves to oppose such evils of a free press as mendacious publication, deliberate falsehood and distortion of facts for political and personal ends."[15] The fight against "mendacious publication," or fraudulent news, as we now term it, is therefore a core component of our core mission, and one that has taken on new urgency in the United States as a confluence of circumstances pose greater threats to the foundations of truth and open discourse in our country. In *Faking News,* we stated that, in "a climate where individuals expect that the information they receive is as likely to be false as true; where they fear that they won't be believed even when they are telling the truth; and where they anticipate being dismissed by anyone not already predisposed to credit their views, free expression cedes its value."[16]

The spread of false information under the guise of news erodes public trust in the news media. This deteriorating trust, and the public's increasing inability to distinguish truth from lies, threaten our democratic discourse. They do so by attacking the shared factual knowledge that undergirds our ability to debate policies, hold government accountable, and identify solutions to the pressing challenges of our time. They also contribute to the spread of extreme ideologies untethered from factual reality. At a time of great polarization and creeping extremism, the threat of fraudulent news is grave.

At the same time, attempts to counter fraudulent news and mitigate its damage, while welcome and necessary, carry their own risks. Under pressure from Congress, governments, and civil

society advocates, tech companies and social media platforms are more eager to fight fraudulent news than they were even a year ago. Having repeatedly been caught flat-footed, they have finally stepped up efforts and are now, in general, quicker to remove disinformation. The potential for overreach, however, is significant. As several examples from the 2018 midterms indicate, even well-intentioned attempts to contain false news can unwittingly curtail free expression rights and enable censorship.

Fighting Fraudulent News: Key Stakeholder Initiatives in the Run-up to the 2018 Midterms

If fraudulent news poses a threat to civic discourse and free expression generally, the stakes are significantly higher in the context of an election. The prevalence and impact of fraudulent news in 2016 were not fully appreciated until months after the fact. Tech companies and other stakeholders have spent the past two years playing catch-up, and they have acknowledged, if belatedly, that they were unprepared. Yet even now that the nature and scope of the challenge are more widely recognized, solutions remain elusive.

In part this is because the problem itself is evolving. While foreign disinformation operations were quieter in 2018 than in 2016, this reduction fails to tell us what to expect for future presidential contests. At the same time, however, fraudulent news has seeped into our domestic discourse, fealty to truth and facts is weakening, and the currency of election-related information is being devalued. With the potency of Russian election-interference operations made plain, domestic actors are drawing from that playbook. A *The New York Times* article comparing disinformation from the 2016 presidential campaign and the 2018 midterms stated, "What is different this time is how domestic sites are emulating the Russian strategy of 2016 by aggressively creating networks of Facebook pages and accounts—many of them fake—that make it appear as if the ideas they are promoting enjoy widespread popularity."[17] And the technology is advancing faster than the solutions, with bots that are increasingly adept at impersonating real people. The ability to target and inundate narrowly tailored categories of voters with intensive floods of selective information means that messages that might once have seemed anodyne or par for the course in a hotly contested campaign have greatly heightened potency to influence opinions and votes. With more sophisticated technical tricks, and with more domestic actors engaging in fraudulent news, the challenge of tackling fraudulent news has never been more urgent, or more difficult.

Tech Companies

Much of the responsibility for addressing fraudulent news—whether during an election cycle or not—lies with the internet giants, particularly Facebook (which additionally owns Instagram and WhatsApp), Google (which owns YouTube), and Twitter. This is in part because Americans rely so heavily on social media as a news source. According to a Pew survey released in September 2018, 68 percent of American adults get at least some news from social media.[18] Facebook is the most common source, with 43 percent getting news from it, whereas 21 percent get news from

YouTube and just 12 percent from Twitter.[19] (These numbers have not changed significantly from 2017.[20]) Notably, of those Americans who get at least some news from social media, 57 percent expect the news found there to be "largely inaccurate."[21]

In our 2017 report *Faking News,* PEN America examined in depth the role that Facebook, Google, and Twitter have played in the spread of fraudulent news, as well as the ways each platform was responding to the problem at the time.[22] We noted that platforms must consider the multiple roles they play in providing information to the public, sometimes providing ostensibly content neutral platforms but at other times creating, aggregating, curating, or elevating content in ways that bleed into the role of a publisher and that inevitably involve some judgment about the content being put forward.

All the platforms face the seemingly contradictory pressures of removing fraudulent information while also protecting free expression and avoiding the role of unaccountable global censor. Overreliance on algorithms and other forms of artificial intelligence (AI) to de-prioritize less trustworthy information, root out fake accounts, or find bots can inexplicably block innocent users or, as Facebook algorithmic changes demonstrated in early 2018, cause news outlets' traffic to plummet for reasons other than a thoughtful assessment that the information they provide is untrustworthy.[23]

Twitter, Google, and Facebook have each been criticized for failing to adequately police their platforms and to prevent Russian interference during in 2016 election, and scrutiny of their platforms has increased significantly since 2017. Executives from the three companies have been repeatedly called before Congress to answer questions about foreign influence operations on the platforms, their commitment to user privacy, the micro-targeting of election ads, and how they would deal with bots, hate speech, and the spread of fraudulent information.[24] And Congress has increasingly hinted at the possibility of regulating social media, potentially by mandating greater transparency, enforcing increased information sharing with the government, creating clearer standards for the protection of user data, or revisiting Section 230 of the Communications Decency Act—a provision that protects platforms from being held liable for content on their platforms.[25]

A series of revelations over the past year has hit Facebook's reputation particularly hard. In March 2018, it was discovered that data analytics firm Cambridge Analytica had harvested data from over 50 million Facebook users without their knowledge and deployed it to profile and target voters in the United States.[26] In November, *The New York Times* reported that, among other efforts to counter negative press, Facebook had "employed a Republican opposition-research firm to discredit activist protesters, in part by linking them to the liberal financier George Soros."[27] In December, the *Times* revealed that Facebook had given other tech giants, including Microsoft, Amazon, and Spotify, "more intrusive access to users' personal data than it has disclosed, effectively exempting those business partners from its usual privacy rules."[28] This included providing Netflix and Spotify access to users' private messages.

These violations of users' trust (and users' agreements) are relevant to the discussion of fraudulent news for several reasons. First of all, user data of this sort could be used to distribute and target fraudulent news more effectively to those most likely to believe it. Second, as PEN America advocated in *Faking News*, tech companies should be more transparent and should

maximize information sharing with researchers, so as to improve understanding about how information is shared and consumed on the platforms.[29] We continue to believe that such transparency is in the best interest of users and companies alike and that it is a critical component of countering fraudulent news. But increasing evidence of how such data has been misused rightfully raises user concerns and puts important, credible collaborations with researchers at risk.

Finally, these scandals also raise urgent questions about the degree to which the companies are equipped to address the grave challenge of fraudulent news. While each has taken steps to combat the abuse of its platform during the midterm elections and beyond, some of these steps have themselves been controversial or had negative repercussions, as discussed below. PEN America believes that digital platforms have a pivotal role to play in curbing the spread of fraudulent news and ensuring the integrity of the digital public square. At the same time, we recognize real risks in empowering private companies to arbitrate massive volumes of speech in ways that are shielded from scrutiny. The tech industry, free expression advocates, election specialists, news organizations, and legislators are at an early, experimental stage when it comes to understanding the problem of how to keep public discourse free and open, and to safeguard democracy, amid these risks. Trial and error, transparency, rigorous scrutiny and criticism, prototyping, research, analysis, and sustained attention provide the only hope of eventually perfecting tools that may sustain what is best about the digital information arena while curbing its most nefarious features.

Facebook

After the 2016 elections, when CEO Mark Zuckerberg was criticized for allowing outsiders to manipulate his platform--which now has 2.3 billion monthly active users--to distribute fraudulent information for political gain, he publicly dismissed this charge as "a pretty crazy idea."[30] As more evidence of significant interference emerged, however, Zuckerberg changed his tune, and in April 2017 Facebook acknowledged that "malicious actors" had created imposter accounts to spread disinformation.[31]

The company stated in a September 2017 blog post that "about 470 inauthentic accounts and Pages" bought roughly 3,000 Facebook ads between June 2015 and May 2017.[32] The accounts and pages were "likely operated out of Russia."[33] The blog post also noted that most of these ads focused not on the election explicitly, but rather "on amplifying divisive social and political messages across the ideological spectrum—touching on topics from LGBT matters to race, immigration, and gun rights."[34] Zuckerberg has said that his company was focused on run-of-the-mill cyberattacks and was ill prepared for well-coordinated foreign information operations spreading divisive disinformation.[35]

In July 2018, Facebook told Congress that it had identified a political influence campaign aimed at Americans that may have been intended to affect the midterm elections.[36] The company announced that it had taken down 32 pages and fake accounts across Facebook and Instagram, created between March 2017 and May 2018, that were engaging in "coordinated inauthentic behavior."[37] At least 290,000 users followed at least one of the pages, and collectively they ran more than 150 ads and created approximately 30 Facebook events.[38] Facebook at the time said it could not determine definitively who was behind the attacks, although it noted that some of

the tactics used were similar to those employed by the Kremlin-linked Internet Research Agency.[39] Nathaniel Gleicher, Facebook's head of cybersecurity policy, noted that the platform observed growing sophistication among those engaging in deceptive behavior online, including using virtual private networks and purchasing ads through third parties.[40]

In an effort to right past wrongs and meet the ongoing threat, Facebook executives told reporters in October 2018 that the company was taking a three-pronged approach to the upcoming elections: tackling fake accounts, limiting their ability to distribute fake news and information, and increasing transparency around political advertising.[41] Accordingly, it has removed fake accounts,[42] marked political ads more clearly,[43] released a searchable ad archive,[44] adjusted its algorithm to downgrade the purveyors of false news,[45] given fact-checkers and researchers greater access to data,[46] and developed information panels that users can open up on their screens to learn about news sources.[47] As will be explored below, some of these initiatives have rolled out more smoothly than others, with several engendering their own controversy and problematic side effects.

Fact-Checking and Downgrading

Most of Facebook's 2018 efforts to fight fraudulent news relied on pre-existing strategies, especially the use of algorithms. Once algorithms determined that an information source would routinely "create or share misinformation," that source automatically lost prominence in users' News Feeds but was not removed entirely from the platform.[48] Algorithms also identified posts with so-called clickbait headlines and pushed them farther down in News Feeds.

PEN America addressed this strategy in depth in *Faking News*.[49] We urged caution for this type of algorithmic downgrading, noting that "adjusting algorithms to de-emphasize or suppress 'low quality' content should be approached carefully and with as much transparency as possible."[50] We did, however, note that from a free speech perspective, downgrading a story was preferable to removing a story entirely. We continue to hold that view today. Still, while Facebook has released information explaining its process for ranking News Feed posts and for determining what should be downgraded,[51] many users probably still don't fully understand this process, and it's difficult to assess the actual impact of downgrading on what an individual user sees.

Since December 2016, Facebook has also used fact-checking to boost the integrity of its News Feed.[52] Facebook now works with a global network of over two dozen third-party fact-checkers, all of them certified through the International Fact-Checking Network, to review and identify false content.[53] As with algorithms, if the fact-checkers found posts to be false, those posts would be downgraded.[54]

In addition to employing algorithms and fact-checkers, Facebook downgraded fraudulent news that was brought to its attention by campaigns themselves. Those who spotted false information could request that the fact-checkers examine it, Katie Harbath, Facebook's global politics and government outreach director, told PEN America.[55] "If the fact-checkers rate it false, we will not remove it," Harbath said.[56] "But we will push it down in the feed. We think people have a right to say the sun rises in west, but they don't have a right on Facebook to amplify it. We err on the side of speech, which gets tricky."[57]

Facebook has tried to make its downgrading more granular and discerning. In October 2018, it announced that it would "downrank" News Feed stories with false headlines, even if the stories they touted weren't wholly false.[58] The company told media outlet Poynter that it had offered new options to its fact-checking partners, allowing them to rate either an entire story or just a headline as false.[59] "The new rating," Poynter reported, "is a result of ongoing confusion among fact-checkers about how to tackle stories that could contain valid factual or analytical content, but are posted with an inaccurate headline on Facebook."[60]

That confusion had come to head a month earlier, when *The Weekly Standard*, then one of Facebook's fact-checking partners, challenged the accuracy of a headline posted on ThinkProgress, a blog maintained by the Democratically aligned Center for American Progress, and ended up downranking the entire article in News Feed.[61] The ThinkProgress article, about Brett M. Kavanaugh's confirmation testimony on *Roe* v. *Wade*, bore the headline "Brett Kavanaugh said he would kill Roe v. Wade last week and almost no one noticed."[62] When *The Weekly Standard*'s fact-checkers rated the article false due to its headline (the article explained that the Supreme Court nominee, in his testimony, was actually making a general point about unenumerated rights that the ThinkProgress piece extrapolated from to predict unstated nuances of his stance on *Roe* v. *Wade*), ThinkProgress claimed that it was being unfairly censored.[63] This dispute helps illustrate a core difficulty with a fact-checkers' approach to fraudulent news: False information and acceptable hyperbole can easily blur together, requiring the fact-checker to make a clear judgment call where no absolute clarity exists.

Weeks before the elections, Facebook announced that it would ban disinformation about voting requirements and would fact-check additional forms of potential voter disinformation.[64] But even as the company has continued to refine its fact-checking approach, hazards remain, particularly because of the time and personnel needed to screen out such information effectively and the inherently subjective nature of determining what constitutes disinformation.[65] "It's clear that even as we continue to improve this program," the company wrote in a blog post in June, "we need solutions beyond fact-checkers."[66]

Facebook's fact-checking network took a credibility hit in early February 2019, when partner Snopes announced that it was withdrawing.[67] A fact-checking site that began in the 1990s by debunking urban legends, Snopes said it was not ruling out the possibility of rejoining the partnership in the future, but that for now it was not in the organization's best interest.[68] Vinny Green, Snopes's vice president of operations, indicated that the rationale for the decision centered around the significant amount of time it took Snopes employees to flag false stories, a heavy lift for an organization with only 16 employees.[69] He reflected that, "It doesn't seem like we're striving to make third-party fact checking more practical for publishers — it seems like we're striving to make it easier for Facebook. At some point, we need to put our foot down and say, 'No. You need to build an API [application programming interface].'"[70]

Critics have also alleged that the partnership—in which Facebook pays fact-checkers for their services—risks compromising fact-checkers' ability to criticize Facebook. Such a concern may also have played a role in Snopes's leaving.[71] Whether Facebook should pay its fact-checking partners is a question with no perfect answer. While the platform's power might make its partners hesitant to condemn it, fact-checking teams require resources to do their jobs.

Regardless, the Snopes departure is a signal that Facebook should listen carefully to the concerns of its fact-checking partners and ensure that their needs are being served or, as Snopes's Green suggests, begin developing mechanisms for fact-checking that do not place the burden on small, external organizations.

ACCOUNT SHUTDOWNS

In its November 2018 Community Standards Enforcement report, Facebook stated that from October 2017 to September 2018, it had disabled over 2.8 billion fake accounts, many of them bots "spreading spam or conducting illicit activities such as scams."[72] In August 2017 Alex Stamos, then Facebook's security chief, said that the platform was shutting down more than two million accounts per day, most of them created by "spammers and fraudsters."[73] While this number incorporates many more categories of so-called infringing content than fraudulent news, it does indicate that account shutdowns are a significant tool that Facebook uses against disinformation.

Account shutdowns are the most visible—and perhaps the most effective—way to respond to fraudulent news. They are also among the most worrying in their potential for censorship.

Critics say that Facebook is not always clear about why it is deleting a page or account. "The work of takedown teams is not transparent," said Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation.[74] "The rules are not enforced across the board. They reflect biases."[75]

In response to these concerns, in May 2018 a collection of civil society groups and academics created the Santa Clara Principles on Transparency and Accountability in Content Moderation.[76] The Santa Clara Principles revolve around three pillars:

- Numbers: Companies should publish the numbers of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines.
- Notice: Companies should provide notice to each user whose content is taken down or whose account is suspended about the reason for the removal or suspension.
- Appeal: Companies should provide a meaningful opportunity for the timely appeal of any content removal or account suspension.[77]

In November 2018, PEN America and other groups called on Facebook to adopt the Santa Clara Principles, arguing that "Facebook remains far behind its competitors when it comes to affording its users due process."[78] Facebook responded with a letter outlining its activities in these areas and citing upcoming efforts, including a planned 2019 consultation with stakeholders.[79] In response to PEN America's request for comment for this report, Facebook declined to comment specifically about committing to the Principles, but stated: "We're committed to continuing to refine our Community Standards and content moderation practices, including in the areas of notice, appeals, and data transparency. We're aligned with the civil society coalition on the high-level principles they've set and have already undertaken much of this work."[80]

One major step that Facebook took recently was to begin creating an Oversight Board for Content Decisions, an oversight body to which users could appeal in the event that their content is removed.[81] In late January of 2019, Facebook announced that it had launched a draft charter for this board, which will reportedly be made up of independent experts empowered to reverse decisions on user content. The draft charter, apparently intended as a starting point for discussion, contains 11 different "suggested approaches" to issues such as the board's composition, powers, and processes.[82] A consultation process will refine this vision before the board is actually created.[83]

We applaud this effort to create a meaningful appeals process for content takedowns, something that the Santa Clara Principles explicitly call for. Still, this proposal has far to go—including through substantive consultation with experts, rights groups, and other stakeholders—before its utility can be meaningfully evaluated.

"Coordinated Inauthentic Behavior"

In articulating the rationale for many of its account shutdowns, Facebook has pointed to its policies against what it calls coordinated inauthentic behavior. Facebook made public its policy against such behavior in April 2018, although a company spokesperson noted to PEN America that authenticity has always been a core part of its platform and a subject of its policies.[84] This category represents a major criterion used by Facebook to define, and subsequently shut down, purveyors of fraudulent news, along with other types of problematic behavior.

Facebook defines "coordinated inauthentic behavior" as "when groups of pages or people work together to mislead others about who they are or what they're doing."[85] As Facebook's Nathaniel Gleicher explains in an organizational video, networks are removed "because of their deceptive behavior; it's not because of the content they're sharing. The posts themselves may not be false and may not go against our community standards."[86] In other words, it is the coordination among these account holders and other facets of their online behavior—rather than the content in and of itself—that violates Facebook's rules and becomes grounds for account shutdowns. Gleicher describes a combination of manual and automated tactics for identifying and removing fraudulent accounts, activity that ramped up as the midterm elections neared.

A month before the election, Facebook announced that it was removing another 559 pages and 251 accounts, some of which had engaged in coordinated inauthentic behavior and some of which were spamming.[87] In a blog post, Facebook noted that while spamming is often economically motivated, rather than politically, spammers are increasingly using "sensational political content" to generate traffic to their sites and garner ad revenue.[88] Gleicher noted in relation to these removals: "If you look at volume, the majority of the information operations we see are domestic actors."[89] The accounts and pages spreading fraudulent and misleading information came from both ends of the political spectrum, including a site called Right Wing News, which had more than 3.1 million Facebook followers when it was deleted, and the left-leaning Reverb Press and the Resistance.[90] Facebook alleged that many of these outlets were using fake accounts to redirect traffic to their websites.[91]

The day before the midterm elections, Facebook revealed that the FBI had tipped it off to a network of activity believed to be linked to "foreign entities."[92] Hours after the polls closed on Election Day, Gleicher released a statement saying that it had responded by removing certain accounts due to "concerns that they were linked to the Russia-based Internet Research Agency (IRA)."[93] In a blog post, Gleicher wrote that "this effort may have been connected to the IRA, but we aren't best placed to say definitively whether that is the case."[94] After further investigation, Facebook announced the next week, it removed a total of 36 accounts, six pages, and 99 Instagram accounts for coordinated inauthentic behavior—although some of these removals appeared to occur after the election.[95] Facebook determined that some 1.25 million people, more than 600,000 of them in the United States, were following at least one of the Instagram accounts.[96] At least some of the content was focused on issues like LGBTQ rights and feminism,[97] and were--Facebook alleged--essentially acting as spam machines that just happen to use political content.

Facebook explained that the content shared by these accounts and pages is "often indistinguishable from legitimate political debate. This is why it is so important we look at these actors' *behavior*—such as whether they're using fake accounts or repeatedly posting spam—rather than their *content* when deciding which of these accounts, Pages or Groups to remove."[98] This challenge becomes even more complicated when the bad actor is not a Kremlin-backed troll but an American whose motives may be more difficult to discern. *The New York Times* reported Gleicher as saying that "the company was struggling with taking down the domestic networks because of the blurry lines between free speech and disinformation."[99]

Facebook's emphasis on addressing behavior, not content, has the clear benefit of allowing the company to avoid being the arbiter of truth, a role that could inevitably lead to censorship. It has the related benefit of insulating Facebook from criticism that it is shutting down pages in a politically biased way. As a private company, Facebook has every right to remove accounts that violate its policies against spamming or fraudulent users.[100] This approach, however, does not necessarily resolve thorny questions around determining which actors are inauthentic.

A recent example of this complexity comes not from the elections but from another highly charged political event. One of the accounts taken down in a series of Facebook actions in July—a left-wing political Facebook page known as Resisters—had created an event page for an upcoming August rally titled No Unite the Right 2—DC, which was ostensibly part of a plan to counter an upcoming white supremacist march.[101] When closing down the Resisters account, Facebook removed the event page, much to the dismay of many legitimate activists involved in planning the protests.[102] Facebook's own blog noted that the Resisters page, though it bore marks of illegitimacy—most notably because a known IRA account had served as an administrator for the Resisters page for a period of 7 minutes—had "connected with admins from five legitimate Pages to co-host the event."[103] The company said that it had contacted the co-hosts and was reaching out to the 2,600 individuals who had expressed interest in the event to let them know the event page had been created by a fake account and had therefore been removed.[104] Chelsea Manning, the activist and former Army soldier who was convicted of leaking hundreds of thousands of U.S. military and diplomatic documents to Wikileaks, was also one of the organizers of the counterprotest, and said that the event did not originate with Resisters and was "real and organic."[105] A local coalition expressed anger with the removal of the event

page, noting that while the event was, in fact, created by Resisters, it was subsequently used for "legitimate protest organizing and promotion" by local organizers.[106]

Chris Metcalf, who operated nine political pages that were deleted by Facebook in October 2018, said that his political speech was also unjustly penalized. "The problem with language like 'inauthentic coordinated behavior' is that everyone in this space coordinates," he told *The Guardian*.[107] "We swap each other's best-performing content . . . But I'm not a bad actor. I'm a legitimate political activist."[108] Matt Mountain (a pseudonym), who operated several left-wing pages that were deleted by Facebook in September, felt that he, too, had done nothing untoward. "When a post did really well on one page and it fit the theme of one of the other pages, I'd share it across them," he said, explaining the motivation for behavior that Facebook saw as an indicator of inauthenticity.[109] Facebook maintains that mass-scale or automated content sharing—or spamming—undermines the integrity of the platform and the user experience, determinations that it is free to make.

Employees of Reverb Press, an alternative news outlet that had hundreds of thousands of followers when its page was taken down in October, similarly decried Facebook's conclusion that its page was acting as a spammer. "My colleagues at Reverb and I were not motivated by money. Facebook is," wrote Marc Belisle, who had previously worked as Reverb's world affairs editor.[110] James Reader, a co-founder of Reverb, wrote on Twitter: "We do not publish fake news. Yes, we share to social media. But that's what publishers do. It's [*sic*] Reverb Press today; Buzzfeed tomorrow."[111] As an outlet, Reverb Press has been ranked by Media Bias/Fact Check as "biased toward liberal causes" but with a "high" degree of factual reporting.[112]

Buzzfeed media editor Craig Silverman noted that it is perhaps too convenient for Facebook to cite "inauthentic behavior" as the motivator for its takedowns. "The removals are part of the company's stepped-up efforts ahead of the midterms and its work to combat misinformation overall," he wrote on Twitter. "But Facebook will always cite spam or account violations as opposed to content issues whenever possible."[113] The implied concern is that Facebook can use inauthenticity as a justification for account removal even when the true reason might be content-based.

Emphasizing behavior over content leaves other issues unresolved as well. Facebook still faces serious concerns, for instance, over how to distinguish financially motivated actors or foreign interference from more authentically motivated domestic political advocacy. "Drawing the line between 'real' and 'inauthentic' views is a difficult enterprise that could put everything from important political parody to genuine but outlandish views on the chopping block," said ACLU attorney Vera Eidelman.[114] "It could also chill individuals who only feel safe speaking out anonymously or pseudonymously."[115]

Some observers, however, still believe Facebook is not doing enough. Nina Jankowicz discovered what she believed to be several fake Facebook profiles dedicated to boosting the 2018 campaign of Massachusetts State Senate candidate V.A. Shiva Ayyadurai and tearing down his opponents. "Over a period of weeks, I watched them," Jankowicz told PEN America.[116] "Anytime the candidate would post anything on his Facebook page, within an hour there would be 60 to 100 individual posts put up by four people."[117] After spending an estimated 60 hours on her detective work, Jankowicz shared her research with Facebook, which removed the fake

pages a week later. This example of false amplification, she noted, was minor compared with the millions of impressions that Russian trolls generate. Facebook, she concluded, is "moving in the right direction," but "too little, too late."[118] The company "should invest more in human contact rather than thinking that AI will save the world."[119] At the same time, this example demonstrates the significant human effort required to investigate even an isolated case of questionable behavior.

War Rooms

In the fall of 2018, in perhaps the most prominent of its tactics for fighting election manipulation, Facebook prepared for the upcoming U.S. and Brazilian elections by setting up a "war room" at its Menlo Park headquarters. An interdisciplinary rapid-response team meant to mobilize a few weeks before critical elections and disband soon after,[120] the war room hunts down disinformation and polices imposter accounts that try to influence voters. Gleicher noted that because war room staff also work with their own teams throughout the company, it serves as a "nerve centre of this much broader effort."[121] Samidh Chakrabarti, Facebook's head of civic engagement, told journalists in September that war room tactics included simulating different scenarios—such as voter suppression operations and the posting of suspicious election-related content —"to test how prepared we are for them."[122]

A strategic response team, set up by Chief Operating Officer Sheryl Sandberg to help her stay on top of potential problems or crises within the company, was also charged with ensuring that election-related threats were identified and addressed quickly. Bloomberg reported that the response team was responsible for coordinating the company's response to an FBI tip about apparent Kremlin-backed Russian troll activity on Facebook and Instagram, leading to the removal of more than 100 accounts just days before the midterms.[123] *The New York Times* noted that it was the first time Facebook had admitted publicly to using government intelligence to respond to an influence operation.[124]

Is it Working?

The important question, of course, is to what extent these actions are having the desired impact of blunting the spread and influence of fraudulent information. One academic research group, a collaboration between researchers from Stanford University and New York University, has documented some encouraging results: In an October 2018 working paper, it revealed that Facebook users' interactions with a set of articles from over 500 sources of false stories dropped significantly after 2016.[125] In contrast, while Twitter had far less engagement with fake news sites—four to six million a month, a range that is significantly lower than Facebook's even after accounting for the size differential between the two platforms—Twitter user interactions with fake news sites continued to grow between 2016 and 2018. Thus, the ratio of Facebook engagement with fraudulent news to Twitter engagement fraudulent news shifted sharply: "from around 45:1 during the election to around 15:1 two years later."[126]

The results, these researchers cautiously posited, suggested that Facebook's changes to address fraudulent news "may have had a meaningful impact."[127] This study, however, ended

more than three months before the 2018 midterms, leaving open the question of whether user interaction with false-story sources may have shot up again as Election Day neared. Facebook has touted two similar studies—one from the University of Michigan and the other from French newspaper *Le Monde*—that came to similar conclusions.[128]

Another study, conducted by a group of political scientists based in four different universities and published in February 2019, concluded that Facebook played less of a role in leading users to fraudulent news sites in 2018 than in 2016, based on the likelihood that an individual had visited Facebook immediately prior to visiting a fraudulent site.[129] Overall, the study's authors concluded that "the proportion of Americans who visited at least one fake news website has declined since the 2016 campaign and that Facebook use is no longer closely linked to fake news exposure," although they reached no conclusion about overall consumption of fraudulent news.[130] Notably, however, they also found that "exposure to fake news and political advertising on Facebook are especially high among engaged partisans — precisely the group that is likely to be especially vulnerable to misinformation. Despite their relatively small numbers, these individuals also play an important role in party coalitions and in public debate about politics, in part by sharing news and information (whether fake or genuine) within their online and offline networks."[131] Combined with what they found to be "significant targeting of ads by respondents' political views,"[132] this suggests that fraudulent news may not need to be as widely accessed to have a significant impact on political discourse.

At the end of 2018, Buzzfeed published a list of the year's 50 "most viral" fake news stories shared on Facebook and assessed the level of audience engagement each achieved. It found that these pieces of viral fraudulent information generated almost as many shares, comments, and reactions as the top 50 such stories had a year earlier, in 2017: 22 million total engagements in 2018, compared with 23.5 million in 2017.[133] The Buzzfeed writers took pains to point out an aspect of the battle against fake news that Facebook's numbers do not capture: the ability of bad actors to simply shift to a new web domain once they've been exposed, a tactic known as "domain hopping" or "domain cycling."[134]

Media researcher Jonathan Albright identified a different tactic adopted by political groups, including those seeking to spread hyper-partisan news or disinformation: transitioning to private Facebook groups, where users can create and share fraudulent claims with relative invisibility.[135] In these private groups, fraudulent news can essentially be incubated before going public. The private nature of these Facebook groups renders their fraudulent claims invisible to the general public, including researchers trying to track the spread of fraudulent news. Albright noted in his research that he "repeatedly encountered examples of extreme content and hate speech that easily violates Facebook's terms of service and community standards," and that some of the earliest posts on Facebook regarding the false rumor that philanthropist George Soros was funding so-called "caravans" of Central American migrants were found in private groups.[136] But, Albright concluded, because of their near invisibility and because the organizers of these sites apparently "know exactly how to game Facebook's platform," these "shadow organization" activities remain unaddressed.[137]

Shadow organizations and domain cycling reveal the cat-and-mouse nature of combating fraudulent news. They also make the effectiveness of Facebook's efforts against them difficult to measure, and any celebratory claims thereof should be viewed with a skeptical eye.

It is worth noting, additionally, that it is difficult to draw broad conclusions from many of the academic studies that examine the scope and scale of fraudulent news on social media. Because there are always limitations on the usage data to which researchers have access, they are typically working with limited information on the subject at hand, and it is difficult for anyone to truly capture the full picture of fraudulent content. "Simply put, no one in this space has yet done the work of defining the scale of the universe of this kind of content…most of these (admirable) studies which try to quantify the scale or spread of misinformation lack a baseline upon which to build their arguments because one doesn't exist," Cameron Hickey, Technology Manager at the Information Disorder Project at the Shorenstein Center at Harvard Kennedy School, told PEN America.[138] Each study also tends to define fraudulent news or disinformation slightly differently. Individual studies may therefore illuminate particular areas of concern or cause for hope, but they all face some inherent limitations that must also be taken into consideration. For the social media platforms, while concerns about user privacy and proprietary information are understandable, the limits on researcher access also provide a convenient basis on which to critique studies they dislike. Increased transparency that allows academic researchers to assess the scale of the problem and also assess the success or failure of efforts to combat it, however, will only help build user trust in the long term.

Twitter

With 321 million active monthly users worldwide[139] and 66 million in the United States,[140] Twitter enjoys influence even beyond these numbers due to its popularity among politicians, celebrities, journalists, and other influencers—most notably President Trump, who relies heavily on the platform to communicate directly with his 58 million followers. As a social media giant, Twitter has also received loud and sustained criticism for the presence of fraudulent news on its site, both in terms of the viral nature of fraudulent stories that spread throughout its platform and in terms of the 'bots', fraudulent accounts that are today well understood to be major vectors for fraudulent news.

Research has increasingly made clear how prevalent fraudulent stories were on Twitter during the 2016 election cycle, and how potentially significant in their effects. An October 2018 study by the Knight Foundation found more than 6 million tweets "linking to fake and conspiracy news publishers in the month before the 2016 election."[141] The authors of the study noted that the significant majority of the accounts who repeatedly linked to such news--including accounts that the study authors argued should fall afoul of Twitters' prohibition against "spammy behavior"--were still active as of spring 2018.[142]

Another study, by Indiana University in November 2018, concluded that fraudulent news was a bigger problem on Twitter during the 2016 election than was originally understood and that Twitter bots played a disproportionate role in spreading misinformation online.[143] The researchers found that just six percent of the bot accounts they identified drove approximately one-third of the "low credibility" information spread throughout the platform.[144] A later study of Twitter during the 2016 election, published in January 2019 in *Science* magazine and undertaken by researchers at Northeastern, Harvard, and SUNY Buffalo, found that "although 6% of people who shared URLs with political content shared content from fake news sources, the vast

majority of fake news shares and exposures were attributable to tiny fractions of the population."[145]

At the same time, Twitter has demonstrated a greater reluctance to take major action than other platforms. In an interview in August 2018, two years after the first reports of Russian interference, CEO Jack Dorsey replied to a question about fraudulent news by saying: "I think what we could do is help provide more context. . . . Also, identifying more credible voices in real time and amplifying that credibility is something we can do. But we have not figured this out, but I do think that it would be dangerous for a company like ours . . . to be arbiters of truth."[146]

As previously noted in our report *Faking News*, Twitter has primarily focused its efforts to counter fraudulent information on activity that violates its terms of service and on identifying and removing fake accounts.[147] In a 2017 blog post about Russian interference in the 2016 elections, Twitter described some of the tools it relies on to identify and prevent suspicious log-in attempts, block content that comes from suspicious or known problematic sources, and look for patterns to spot "non-human activity."[148] The post went on to explain the added difficulty of identifying coordinated human activity and noted that when fighting it, "the risks of inadvertently silencing legitimate activity are much higher."[149]

According to the Twitter Rules, users may not "use misleading account information in order to engage in spamming, abusive, or disruptive behavior, including attempts to manipulate the conversations on Twitter."[150] Suspicious behavior includes the "use of stock or stolen avatar photos; use of stolen or copied profile bios; use of intentionally misleading profile information, including profile location."[151] In June 2018, Twitter said it was focusing on "developing machine learning tools that identify and take action on networks of spammy or automated accounts automatically."[152] In October 2018, in an update on its efforts to protect election integrity, Twitter noted that it "now may remove fake accounts engaged in a variety of emergent, malicious behaviors."[153] In a Retrospective Review of the 2018 midterm elections, published on January 31, 2019, Twitter stressed that if an entity has been in violation of the Twitter Rules, the company will "remove additional accounts associated with that entity."[154] The rules also lay out the factors that will cause an account to be identified as spam, and they prohibit the sharing of hacked information.[155]

Twitter has primarily offered the sheer number of "spammy and automated" accounts identified by its automated detection mechanism as evidence of the mechanisms success, but without providing details on its accuracy.[156] This was true in the June 26 blog post, and in the Retrospective Review the company noted: "We are now removing 214% more accounts year-over-year for violating our service manipulation policies."[157] To its credit, however, starting in October 2018 Twitter started making publicly available data sets of accounts and content related to possible information operations, so that researchers can study and better understand such activities.[158]

Twitter's campaign against fraudulent accounts ramped up significantly in 2018. Between May and June, the platform suspended more than 70 million accounts that it suspected were false or suspicious, according to data obtained by *The Washington Post*—a whopping one-fifth of its reported 336 million monthly active users[159]—after determining that they were created by bots

rather than real people. In the spring of 2018, Twitter was suspending more than one million accounts a day.[160]

This widespread cleanup has been cautiously welcomed by some commentators as potentially contributing to a more fact-based and authentic platform during the 2018 election season. "Twitter is doing a slightly better job this campaign season," Nina Jankowicz told PEN America in October 2018.[161] "I might say that because they made a good-faith effort to reach out to people like me who study them. But they have been aggressive about taking down accounts."[162]

In an update posted in October, Twitter said that it was continuing "to enforce our rules against intentionally misleading election-related content" and described the creation of an election-specific support portal to provide prompt support to "electoral institutions."[163] In its Retrospective Review, the company described this so-called partner support portal in more detail, stating that its goal was to "expedite our response to reports from people and organizations active in the election arena. This includes election support organizations, U.S.–based research organizations, and universities and academics who study the spread of misinformation in the media."[164] Twitter noted that its more than 10 partners included the Republican National Committee, the Democratic National Committee, the National Association of Secretaries of State, and the National Association of State Election Directors.[165] The company reported receiving 43 reports via the portal, "resulting in the removal of thousands of accounts and Tweets in violation of our rules."[166]

Twitter's October post specifically referenced the removal in August of 50 accounts—reportedly run by individuals in the United States—that were posing as representatives of various state Republican parties and stated that Twitter was partnering closely with the Republican and Democratic National Campaign Committees and with state election offices to address imposter accounts and election-specific disinformation.[167] In the same post, Twitter revealed the removal in August of another 770 accounts that it believed were engaging in coordinated behavior and had originated in Iran.[168]

Shortly before the election, Twitter confirmed that it had removed over 10,000 automated accounts that were posing as Democrats and discouraging people from voting.[169] The Democratic Congressional Campaign Committee (DCCC), which works to elect Democrats to the U.S. House of Representatives, flagged the activity for Twitter.[170]

In its Retrospective Review, Twitter noted that it had also made internal structural changes to better prepare for the midterm elections. These included the creation of a "cross-functional analytical team whose mission is to monitor site and service integrity."[171] Twitter stated that:

> The primary focus of the cross-functional analytical team is election readiness. Leading up to and during the 2018 election period, the team examined, responded to, and escalated instances of suspected inauthentic, election-related coordinated activity in political conversation . . . [The] cross-functional team developed a political conversations dashboard to surface information about sudden shifts in sentiment around a specific conversation, suggesting a potential coordinated campaign of activity, as well as information about groups of potentially linked accounts that are posting about the same

> topic. . . . Accounts were escalated for review in real time if exhibiting anomalous patterns of behavior.[172]

To further defend against imposter accounts and help users determine whether they are legitimate, in May Twitter announced "election labels" for verified candidates running in the 2018 midterms.[173] The label was available only for candidates running in gubernatorial or U.S. House or Senate races during the 2018 November midterm general-election cycle. Similar to the platform's blue checkmark, which indicates that an account has been verified, a small gray icon of a government building, with text identifying the candidate's state and the office being sought, appeared on a verified candidate's Twitter profile page, in all tweets and retweets, and in tweets embedded in stories and articles published outside Twitter. To validate accounts, Twitter partnered with Ballotpedia, a nonprofit that publishes nonpartisan federal, state, and local election information. Once candidates qualified for the November general election ballot, their Twitter accounts were automatically authenticated with the government building icon, and candidates were given seven days to opt out.[174] Twitter reported that it identified 1,025 candidate accounts and provided labels for 95 percent of them.[175] This logical and constructive initiative provided a simple means of helping the public identify official sources of information.

Not all of Twitter's efforts have gone as smoothly, however. On October 30, the platform launched a midterm-elections-focused events page[176] to help users keep track of news and information. While well-intentioned, it quickly went terribly wrong. Hours after the page's launch, BuzzFeed reported that it was filled with conspiracy theories and false, hyper-partisan news.[177] A Twitter spokesperson told BuzzFeed that the page's algorithm pulled tweets based on keyword, automatically presenting content associated with those keywords.[178] Some content shown to an individual Twitter user was based on accounts that user follows, making it more likely that someone who follows, say, conspiracy theorists, would see related conspiratorial content. A significant amount of content on the events page was low quality or actual disinformation, including a claim that the GOP gubernatorial candidate in New York had dropped out of the race and unfounded claims of illegal voting.[179] Many of the accounts featured also appeared to be fake.[180] Given that the page was driven by algorithms and would reflect an individual user's own information bubble, Twitter might have taken more care in promoting the page as a source of "the latest news and top commentary" on the elections.[181] As noted in *Faking News*, social media platforms incur added obligations for scrutiny and verification when content is not simply posted by users but rather collated and republished by the platform itself under a news or information rubric that implies such information is credible.[182]

Unlike Facebook and Google, Twitter apparently did not pursue options for integrating fact-checking into its platform before the election. In a December 2018 article, the media-news site Poynter noted that "Twitter has stepped up the removal of false accounts, but has not put in place a more systemic response to virally false tweets,"[183] and predicted that it might take steps to catch up with the other platforms at some point in 2019—too late for the 2018 election cycle but perhaps with an eye toward 2020.

For all Twitter's efforts, just a week before the election, researchers from Oxford University reported that the platform had 5 percent more false information circulating than it did during the 2016 election.[184] While the Oxford study might have inflated the number of "junk news" sites by including unreliable and hyper-partisan sites that also present factual information in that

category, the report concluded that Twitter users circulated higher proportions of news from sites known more for conspiracy mongering and hyper-partisanship than from traditional sources.[185] Twitter's head of site integrity, Yoel Roth, contested the accuracy of the report in a tweet, saying that the research methodology was "deeply flawed" because it was based purely on publicly available information, which could result in a "staggering margin of error."[186] Nonetheless, the findings still point to the whack-a-mole nature of Twitter's battle against bots.

Google and YouTube

While Google and its subsidiary YouTube have faced somewhat less scrutiny than Facebook and Twitter for spreading false information, they have not escaped altogether. Most notably, Google's failure to send a senior executive to a Senate Intelligence Committee hearing on election security in September 2018 frustrated lawmakers, who left a chair empty next to Sheryl Sandberg, Facebook's COO, and Jack Dorsey, Twitter's CEO, to mark the absence.[187] Without Google there to respond, senators expressed concern about Google Search "surfacing absurd conspiracies," and "Russian-backed disinformation agents" spreading divisive videos on YouTube.[188]

As a search engine, not a social media platform, Google does experience different issues with disinformation. When Sundar Pichai, Google's CEO, eventually appeared before Congress, in December 2018, he pointed to the essential algorithmic nature of its search engine as an inherent constraint on how much control the company could extend over fraudulent stories.[189] If a lot of people click on a fraudulent search result, Google's algorithms naturally rank that result higher in search rankings, a process that allows information that is fraudulent but of great interest to users to rise to the top.

In addition to running the world's biggest search engine, Google runs its subsidiary, YouTube, the mega video-sharing site.[190] In October, during a congressional hearing, Google downplayed YouTube's role in enabling Russian election interference.[191] But the video platform has extensively spread false information, conspiracies, and hoaxes. The prominence of videos promoting conspiracy theories and inaccurate information in the wake of mass shootings[192] in Parkland, Florida, and Las Vegas in 2018 highlighted the problem. In July, YouTube said that it would work harder to surface authoritative results, particularly during breaking news incidents,[193] and in January 2019 the company announced that it would alter its algorithms to stop recommending fraudulent information and conspiracy theories.[194] While such videos would still be available on YouTube, they should become less likely to be recommended to users who have not sought them out.

Because Google's platform is so algorithm-centric, the company's efforts to combat disinformation have relied on tweaking these algorithms to reduce the prominence of fraudulent information in search results. Since 2017, in response to the 2016 election, Google has also highlighted fact checks in search.[195] If a fact check from a qualified source exists for a search result, the user will see a "fact check" label and a box with information on "the claim being checked; who made the claim; the name of the publisher doing the fact check; a summary of the publisher's fact check."[196] Google relies on several factors to determine whether a fact-checker is trustworthy and is clear about what it considers a legitimate fact check.[197] But this

determination is made in part by an algorithm, the details of which Google has not shared, although it has said that there are "about 200 signals of quality that factor into the algorithm's decision."[198] The impact of these efforts has not yet been thoroughly evaluated.[199] Google's concerns about sharing any details of its algorithm limit the ability of outside researchers to assess the impacts of measures the company takes. Google has also begun reducing the number of tweets that appear in Google search results, out of recognition that Twitter, too, is vulnerable to manipulation.[200]

In late 2017, Google introduced a new feature to evaluate a news outlet's reliability in its "Knowledge Panels," the box that shows up on a search page with a summary of information. For news publishers, a tab for "reviewed claims" would show up "when a significant amount of a publisher's recent content was disputed and reviewed by an authoritative fact-checker."[201] But the feature drew criticism from conservative outlets like The Daily Caller, which claimed bias because it received "reviewed claims" tags while explicitly liberal sites like Daily Kos and ThinkProgress did not.[202] Google suspended the initiative in late January 2018.[203] Although "reviewed claims" are still described on the help page, Google does not appear to have reinstated the initiative.[204]

The company is also building a dedicated fact-checking search engine, intended to make it easier to find all the checks that exist on a certain topic. It remains in beta form, accessible only to select fact-checkers or journalists, but Google has stated its intention to open it to the public in 2019.[205]

In a blog post on August 23, 2018, Kent Walker, Google's senior vice president of global affairs, wrote that the company's Threat Analysis Group was working with its Trust and Safety team and with Jigsaw, an incubator under Google's parent company, Alphabet Inc., to identify bad actors, disable their accounts, warn users, and share intelligence with both other companies and law enforcement.[206] In that post, titled "An update on state-sponsored activity," Walker went on to describe influence operations tied to the Islamic Republic of Iran Broadcasting (IRIB) that were identified through Google's partnership with cybersecurity company FireEye, as well as ongoing efforts against people connected to the Russia-based Internet Research Agency.[207] While the post was somewhat vague about the exact nature of these operations, it did refer to "political content" in both cases. It also reported taking down, as of November 20, 2018, a total of 73 YouTube channels, seven blogs on its Blogger platform, and 19 Google+ accounts in connection with the IRIB organization, and 43 YouTube channels and one blog connected to IRA operations.[208]

In March 2018, Google launched the Google News Initiative, describing it as an effort to work with the news industry to help journalism thrive in the digital age.[209] Its aim, according to the company's announcement, is to elevate accurate news during breaking news events; to collaborate with newsrooms, civil society, and fact-checkers to foster trust and accuracy in news; and to support media literacy for young people.[210] The initiative includes partnerships with news outlets, as well as the development of products and programs to support news outlets and the news industry.[211] Google appears to envision the program as key to stemming the flow of disinformation on the internet, though some have interpreted it as a way to blunt criticisms that Google and Facebook's dominance of the online advertising market has starved news organizations of the resources they need to survive.

The announcement of the Initiative included a pledge to spend $300 million over the next three years to support "authoritative journalism."[212] During the midterms the program helped local journalists report on the elections by providing trends and state-level data to journalists to see which issues voters in their region were most focused on.[213] "For election reporters based in the United States, it's one way to find out what their readers care about through real-time search data," a September Google blog post said.[214] To facilitate accurate reporting, the Election Databot, a Google partnership with the website ProPublica, pulled together local election data, including "Google Trends data, candidate spending data, campaign ads, deleted Tweets, and campaign statements."[215] Google is also working with nonprofit partners—from the anti-disinformation organization First Draft to the collaborative newsroom Cross Check and the civil society booster Trust Project—to provide resources for ferreting out and eliminating disinformation.[216]

Making Political Ads More Transparent

Google, Twitter, and Facebook all sell political ads, and in 2016 foreign agents used these platforms' ad services to spread disinformation, sow dissension, and suppress voter turnout.[217] Facebook admitted in a September 2017 blog post that between June 2015 and May 2017 it had sold more than $100,000 worth of political ads connected with fake accounts likely operating from Russia and that these accounts generally aimed to "amplify divisive social and political messages."[218] The company turned over information behind those ads to congressional committees investigating Russian influence operations in the 2016 elections and to Special Counsel Robert Mueller.[219] The Senate report published in December 2018 noted that "73 different IRA-affiliated [Facebook] Pages and Instagram accounts were part of an ads operation that consisted of 3519 ads."[220] Facebook has come under particular fire because its micro-targeting capabilities allow advertisers to direct their messages to very specific subsets of people and to modify the ads in real time so that they can hone in further and become even more effective. Research shows that the Kremlin-backed IRA used these tools to send messages to voters of color, discouraging them from voting.[221]

In October 2017, Senator Amy Klobuchar, with Senators Mark Warner and John McCain, introduced the Honest Ads Act, which would require online political ads to be covered by the same rules as those sold for TV, radio, or satellite.[222] While Facebook and Twitter have publicly backed the bill,[223] some critics have argued that tech giants would rather deflect such regulation. "Privately," said Michael Posner, director of the NYU Stern Center for Business and Human Rights, "they've made it clear they are not for it."[224]

In response to PEN America's request for comment for this report, Google, Twitter, and Facebook all disputed such a characterization. Google provided the following statement: "We are committed to working with legislators to deter foreign governments from using any communications platform to influence US elections, and to ensure greater transparency in online political advertising generally."[225] Facebook responded by referencing Zuckerberg's publicly stated support for the bill, and stated the company "continue[s] to believe that it represents an important step in tackling the industry-wide challenge of preventing foreign election interference."[226] Twitter responded by saying that allegations that Twitter does not

support the Act are "entirely inaccurate," with a spokesperson elaborating that "Twitter publicly supported the Honest Ads Act in April 2018 and we remain supportive."[227]

In the 2018 midterm election cycle, Facebook, Google, and Twitter took steps to make their political ad[228] sales more transparent and to more clearly label the ads.[229] All three put in place clear requirements for political advertisers to confirm their identities and their locations in the United States, with Facebook and Twitter requiring advertisers applying for verification to receive a letter at a U.S. mailing address.[230] Facebook and Twitter apply the same requirements to issue ads, which do not promote particular candidates but do advocate on political issues.[231] All three platforms include "paid for by" information on the ads.

But so far, Facebook's efforts to verify its political advertisers have fallen woefully short. Authorized advertisers have been free to fill in the "paid for by" disclaimer with whatever description they choose, without verification. The result has been that once advertisers were authorized, they had carte blanche to disguise their identities. And at least a portion of such advertisers apparently used disguises to deliberately mislead users about the source of the advertisements they were viewing.

Those aiming to prove the flimsiness of Facebook's purported safeguards have not had to work hard. A November 2018 ProPublica investigation found dozens of examples of Facebook's "paid for by" label being manipulated so that posts of unknown origin appeared to be associated with candidates, campaigns, or official political groups.[232] Similarly, Vice News revealed in October that it had applied and been approved to buy political ads on Facebook while claiming they were "paid for by" ISIS and Vice President Mike Pence (an ad "paid for by" Hillary Clinton was rejected).[233] Vice was also able to place ads that were exact replicas of some posted by Russians in 2016.[234] It went through Facebook's advertiser authorization process, including the verification of a home address. As Vice pointed out, "That meant Facebook knew who was behind the ads internally, but externally, Facebook users would see [what] was completely made up Paid For information."[235] Facebook acknowledged that the ads should not have been approved. "Enforcement isn't perfect," an official said, but "we have made it much harder" to abuse the system "and we will continue to improve."[236]

After succeeding in placing these ads, Vice posed as all 100 U.S. senators to see if it could be approved to buy political ads on their behalf. Facebook granted approval in every case.[237]

In October, the news site Business Insider revealed that it, too, had conducted a political-ad experiment. It ran two ads on Facebook that were labeled as being "paid for by Cambridge Analytica," the company that was implicated in a massive Facebook data breach scandal and was subsequently banned from the platform.[238] Facebook confirmed that the ads had run despite the ban but did not explain why. Its website states that ads are subject to review by a combination of artificial intelligence and human analysis.[239]

Weak enforcement is not unique to Facebook. A group posing as Russian trolls found it equally easy to buy ads on Google—it did so from a location inside Russia and paid with rubles.[240] Researchers from the Campaign for Accountability, an advocacy group, announced in September that they had successfully bought political ads on Google using fake profiles intended to look as if they were affiliated with the Internet Research Agency; the ads used

content used by the IRA in 2016.[241] Even evoking the most notorious source of Russian propaganda somehow failed to set off alarm bells for Google. The ads also appeared on YouTube and on the websites of CNN, *CBS This Morning*, HuffPost, and The Daily Beast. Google responded to Buzzfeed's revelations by saying that it was taking "further appropriate action to upgrade our systems and processes."[242]

Disclosure of corporate or other foreign political funding is essential to combat election-distorting disinformation campaigns. But it does not wholly solve the problem. Legislative solutions like the Honest Ads Act and the recently introduced For the People Act—a comprehensive election reform bill that includes the provisions of the Honest Ads Act[243]—are good starting points, as long as they do not create perverse incentives that would drive online platforms to be overly restrictive in what ads they permit on their platforms.

Legislative Proposals for the Online Disclosure of Political Ad Funding

The Federal Elections Campaign Act (FECA), which regulates political campaign fundraising and spending, was passed nearly 50 years ago in a drastically different political and communications landscape. The act restricted the amounts that donors could contribute to federal candidates and parties and mandated the disclosure of contributions and expenditures in campaigns for federal office. FECA has been revised several times over the years. Most recently, there have been efforts to bring the advertising disclosure provisions into the digital age to hold online political ad funding accountable to the same standards as print and television media.

As news consumption has moved online, policy makers have sought to expand FECA accordingly. Bills such as the Honest Ads Act, introduced in the Senate in 2017, would extend the existing requirements for the disclosure of funders of political advertising, which currently apply to print, television, and broadcast communications, to apply online.[244] Companies that publish political ads would be required to maintain copies of these ads and disclose how much was spent on each one as well as how and to whom it was targeted.[245] The ads to be covered by the bill would include any that:

> (i) is made by or on behalf of a candidate; or
> (ii) communicates a message relating to any political matter of national importance, including—
> (I) a candidate;
> (II) any election to Federal office; or
> (III) a national legislative issue of public importance.[246]

The inclusion of ads relating to "national legislative issue[s] of public importance" represents a broadening of the set of ads that would be regulated online. In 2018, when Facebook attempted to roll out some elements of the Honest Ads Act of its own accord, issue ads—touching on matters like immigration, gun control, and criminal justice—proved challenging to regulate properly (see "Spotlight: Ad Policies and Publishers," below). The breadth of that category raises concerns that the terms of the Honest Ads Act as currently drafted might not be specific enough to hone in on political advertising and avoid ensnaring other types of content.

The newly seated House of Representatives in the 115th Congress has introduced the sweeping H.R. 1, the For the People Act, which includes a newer iteration of the Honest Ads Act as one component. In the bill's words: "The dramatic increase in digital political advertisements, and the growing centrality of online platforms in the lives of Americans, requires the Congress and the Federal Election Commission to take meaningful action to ensure that laws and regulations provide the accountability and transparency that [are] fundamental to our democracy."[247]

H.R. 1 would also task the executive branch with creation of a national strategy to "protect against cyber attacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of United States democratic institutions." Additionally, it would establish a congressional commission to "counter efforts to undermine democratic institutions within the United States."[248] The commission would have 18 months to investigate and research relevant threats and develop a report and set of recommendations for the president and Congress.[249] The proposal for such a national strategy is well warranted. However, it is worth noting that the year-long timeline provided for the strategy's completion almost ensures that this strategy would not be released in advance of the 2020 elections, let alone any of its recommendations implemented. As of the writing of this report, none of the federal legislative proposals requiring the online disclosure of political ads have become law.

Days before this report's release, on March 8, 2019, the House of Representatives passed the For the People Act, moving the bill forward substantially.[250] However, the Act appears likely to stall in the Senate, where the Senate Majority leader, Mitch McConnell, has pledged not to take up the proposal.[251]

Online users—and the American voting public—should be equipped to assess the reliability of the content they consume online. PEN America therefore supports the principle of increased transparency around the funding of political ads, as it allows the public to make informed political choices and hold elected officials accountable. However, as with all such legislation, PEN America cautions that the scope of regulation must be narrow and precisely defined to comport with the First Amendment. Otherwise legislation risks incentivizing overly aggressive actions by the technology companies to ensure adherence and avoid penalties. If legislators are serious about increasing transparency around political ads, they should introduce a standalone proposal that could garner bipartisan support, focusing narrowly on ads relating to candidates and elections. While strategy development is also important to understand the scope of the disinformation problem, it must not preclude actions needed more urgently.

Ad Archives

Facebook, Google, and Twitter each introduced a searchable ad database in the past year. Facebook unveiled its Ad Archive in April,[252] Twitter its Ads Transparency Center in June,[253] and Google its Ad Library in August.[254] The databases provide different categories of information and levels of detail about the ads.[255] But all three contain each ad's sponsor, how much it cost to post, when it was shown, and how many times.[256] All three allow users to swim through their ad pools and search past and current campaign ads running throughout the United States. And all three represent a step forward, though each has notable limits in the

transparency and comprehensiveness of the data shared with the public. As a result, the public response to these efforts has been mixed, with many seeing them as a significant step but still far from sufficient.

In May, ProPublica poked holes in Facebook's political ad system, noting that it relies on a combination of applicants' "voluntary disclosure" and Facebook's algorithmically and manually mining ad buys to determine which are political yet not registered as such.[257] Reviewing the three databases, Natasha Singer of *The New York Times* included lengthy descriptions of the alleged shortcomings of each: "The Facebook archive does not show which campaigns are the biggest spenders or allow you to search ads by date. . . . The Google archive does not show political ads for candidates in state elections or ads on political issues. . . . For state or local political ads on Twitter, you can see only current ads—and those don't include demographic audience data or spending data."[258] Facebook's archive provides estimated data on the age, gender, and location of those who saw the ad, but does not include complete information on how the ad was targeted (although sometimes that can be inferred from the audience demographic data).

In January 2019, ProPublica reported that Facebook had blocked a tool the news outlet developed to show how users were being targeted by political ads.[259] Users could voluntarily install a plugin developed by ProPublica that records data on the ads in their News Feed and information on why they were targeted (information a user can find by selecting 'Why am I seeing this?' on an individual ad). ProPublica used this information to build its own political ad database, allowing people to see more clearly how these ads were being targeted.[260] ProPublica, as well as Mozilla and WhoTargetsMe, two other organizations engaged in similar transparency initiatives, all found their tools stopped working in January, after Facebook made changes that allegedly blocked them.[261] In a statement to ProPublica, Facebook spokesperson Beth Gautier said, "This was a routine update and applied to ad blocking and ad scraping plugins, which can expose people's information to bad actors in ways they did not expect."[262] While Facebook is allegedly developing its own tool to help researchers analyze political ads, and while some caution regarding outside efforts to collect user data is understandable in the wake of the Cambridge Analytica revelations, these developments raise concerns that Facebook is trying to limit independent analysis and control what information credible researchers can access.[263]

In an April statement, Senator Klobuchar argued that the tech companies' efforts are insufficient unless backed by legislative regulation: "This is a positive step by Facebook to take the lead to put in place the transparency requirements called for in the Honest Ads Act, but a patchwork of voluntary measures from tech companies isn't going to cut it—we need to pass the Honest Ads Act. The goal of this legislation is to ensure that all major platforms that sell political advertisements are held to the same rules of the road."[264]

Klobuchar is right: Piecemeal efforts governed by the discretion of the technology companies have not come close to reaching the level of comprehensiveness and effectiveness necessary to curtail fraudulent news and safeguard election-related discourse. Legislation that preserves free expression and focuses narrowly on elections and campaigns could help increase transparency and equip voters with the information needed to assess the credibility of political ads.

SPOTLIGHT: AD POLICIES AND PUBLISHERS

Some of these steps to curb advertising disinformation—particularly Facebook's policies for issue ads—have given rise to a host of unintended consequences and garnered significant blowback. Giving attention to issue ads under these policies is potentially important, since they are the ads most likely to be used to foster division or target specific communities, including around voting. Even so, Facebook's definition in 2018 of what constituted an "issue ad" was overbroad, sweeping up an array of content not germane to the initiative's objectives.

In April 2018, when it announced its new policy for political ads, Facebook's definition encompassed any ad touching on a long list of "national issues of public importance," including civil rights, education, foreign policy, government reform, guns, health, and values—the last of which could essentially capture nearly anything.[265] While Facebook is right that ads that relate to these topics may well be political in nature, that is not always the case. This definition swept up ads from news publishers, nonprofit organizations, and a range of other entities seeking to promote their work on these issues. As a result, when posters sought to boost their news content in those areas by reposting it as paid advertising, their ads were rejected. If trained, qualified individuals had been reviewing these ads earlier in the process and researching their sponsors as necessary, they may have been more able to make obvious distinctions between the work of nonpartisan nonprofits and publishers and the work of political campaigns and action groups.

A June 2018 Poynter article described how the publishers of an article about the mistreatment of migrant children were rejected when they tried to spend $150 to promote the article on Facebook.[266] There were told that they would have to register, or "authenticate," and that the content would have to be labeled as a political ad.[267] As ProPublica pointed out, not only was the policy mislabeling and ensnaring news articles; it was also failing to capture some actual political ads, including one promoting a yes vote on a San Francisco area ballot proposition.[268]

A similar story in July, from KPBS, a San Diego public radio station, told of a five-year-old girl who was forced to appear in immigration court unaccompanied.[269] Under Facebook's new policy, the story could not be boosted to reach a larger audience. In response, Jean Guerrerro, who reported and wrote the story, retorted that now "balanced journalism is now 'political content.'"[270]

In response, Facebook noted that publishers could go through its authorization process to prevent their content from being rejected. Thereafter, though, news articles or other content that they were paying to promote would be labeled as political ads and be included in the political ad archive. For journalists, nonprofit organizations, and others, this was overly restrictive, and troubling in its attempt to mark civic speech and journalism as the equivalent of political advertising.[271]

The *Financial Times* and New York Media were among those that canceled their Facebook advertising in response to the new policy.[272] In June, a coalition of seven media associations, including the American Society of News Editors, the Society of Professional Journalists, and the News Media Alliance, sent a joint letter to Facebook protesting the policy and highlighting the

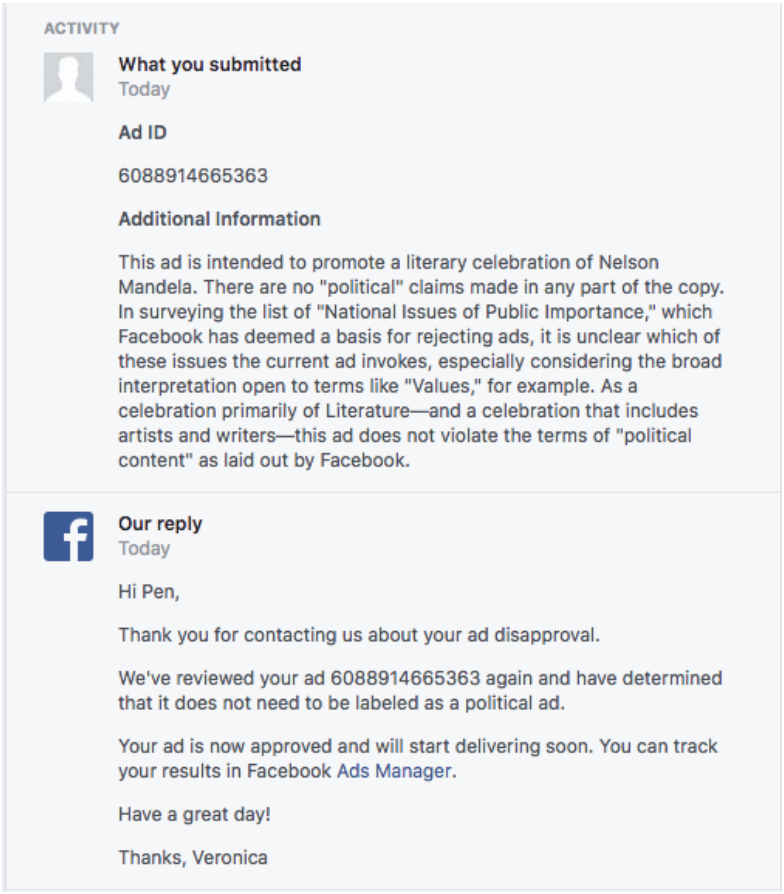
risk it posed to professional journalism.[273] In the letter, the associations said that they viewed the policy as "another step toward furthering a false and dangerous narrative that blurs the lines between real reporting from the professional media and propaganda," and called on Facebook to provide a "clear exemption for publishers of professional journalism."[274]

Maribel Perez Wadsworth, president of the USA Today Network and publisher of *USA Today*, said, "In spirit, what Facebook is trying to accomplish is both reasonable and important—to help their users understand the sources of political advertising vying for their attention. . . . The problem rests in the execution. Facebook's approach fails to draw a critical distinction between journalism and political advertising."[275] Jon Slade, chief commercial officer for the *Financial Times*, said on a podcast that "it is dangerous to describe journalism as political content. Journalism is journalism, and political lobbying is political lobbying. To conflate the two is an extremely dangerous precedent, particularly in this era when there are so many question marks about the veracity of news."[276]

With these concerns in mind, in late June Facebook did adjust its policy to create a separate section in the ad archive for news stories,[277] though publishers found this step insufficient, as the database was still titled "Archive of Ads with Political Content."[278] The website is currently entitled merely "Ad Archive," and invites the user to search ads "related to politics or issues of national importance," while search results can be filtered by "news" vs. "political and issue."[279] When Twitter released its own issue ad policy a few months after Facebook, it built in an exception for news outlets and received a generally appreciative response from publishers.[280]

PEN America had its own experience with the Facebook ad policy. As a nonprofit organization that hosts public programs, we at times utilize Facebook to help promote our events and build audiences, paying to promote Facebook posts for upcoming events. In June 2018, shortly after the policy was altered, Facebook rejected PEN America's post promoting an event of readings and song in honor of the 100th anniversary of the birth of Nelson Mandela and the release of a new volume of his prison letters due to "political content." After PEN America staff submitted an appeal and Facebook carried out a review, it admitted that the determination was made in error and approved the ad. The integration of human judgment earlier on in the process would help avoid such errors and prevent needless and time-consuming appeals.

Source: Facebook



Source: PEN America

Collectively, the ad policies are a prime example of how the pressure on major tech companies to address past and prevent future abuses, while necessary, also puts them at risk of establishing flawed, seemingly rushed polices without fully considering the consequences or engaging in the necessary consultation with human rather than artificial intelligence. As the 2020 elections loom, the risks of overreaction and overreach will only grow. To avoid repeated missteps and further breakdowns of trust, the tech companies must prioritize human engagement with the stakeholders affected by any major policy decision and with the range of content shared on the platform. Ongoing vigilance from civil society groups and the media is also necessary to track these changes and their implications, and to engage with the tech companies to find solutions that broaden the space for online expression, rather than narrowing it.

Tech Company Collaboration with U.S. Government Agencies

Both Google and Twitter have recently touted their collaboration with government agencies as part of their efforts to identify and combat disinformation on their platforms. After the midterms, Facebook announced that it had been working closely on enforcement with, among others, the FBI and the Department of Homeland Security (DHS), which possess "additional tools to deter or punish abuse."[281] The company also reportedly worked with state election boards to notify them promptly of irregularities.[282]

In its Retrospective Review of the midterm elections, Twitter described its "well-established" relationships with agencies, including the FBI's Foreign Influence Task Force and DHS's Election Security Task Force.[283] In November, a Twitter spokesperson noted that the company had "established open lines of communication and direct, easy escalation paths for state election officials, DHS, and campaign organizations from both major parties."[284] The subsequent review described Twitter's Election Day participation in an operations center convened by DHS and comprising participants from the FBI, the Department of Justice, the director of national intelligence, and "federal, state, local, and private sector partners."[285] Shortly after the election, a Twitter spokesperson said, "It was evident on Election Day that we were more efficiently able to combat threats to information integrity through these partnerships."[286]

The motivation for social media companies to engage with law enforcement and intelligence agencies is clear, and in the face of foreign actors attempting to undermine U.S. elections, such coordination is necessary. But it is not without risks. Facebook, with its more than 2 billion users, is perhaps the world's largest platform for public speech, and it has access to extensive user data and billions of private messages between its users. Twitter, with over 300 million users as well as a trove of private inter-user communications, is in a similar position. Given these companies' enormous power, their collaboration with some of the country's most formidable agencies must be zealously evaluated and monitored.[287]

The nature of the coordination between federal law enforcement and the tech companies is murky and will probably remain so. It raises potential concerns for free expression, particularly given repeated and recent revelations about tech companies' lax approach to protecting user data and privacy. In a blog post after the elections, Facebook described the "complexities and

challenges" of coordinating with law enforcement and said that it uses a "rigorous vetting process" when assessing whether and what information to share with the government.[288] The post's assurances that Facebook is careful about users' privacy were vague, and rang rather hollow given the long history of gaps in the company's safeguards.

PEN America reached out to Facebook, Twitter, and Google to ask for more information about their collaboration with government agencies and about their internal policies to protect user privacy and free speech during these collaborations. Google responded by saying, "Google worked with government election integrity task forces ahead of the 2018 elections to better understand the threat landscape to protect our users, and the public generally, and to prevent our systems from being abused. . . . In these election-related engagements with government, as with all such engagements, Google applied its policies to respect the privacy and security of user data. No exceptions were made by Google nor were they sought by government."[289] Google also referenced its Transparency Report, in regards to our question about the public accessibility of information around such collaborations.[290]

Facebook, in its response, pointed to its participation in the Global Network Initiative, a multi-stakeholder initiative that develops principles and guidelines for companies to adhere during their activities. The guidelines take on human rights and other corporate responsibilities (PEN America is also a member of the GNI). Facebook noted that these guidelines "directly address practices for responding to requests from law enforcement and national security agencies that may implicate user privacy and freedom of expression."[291] Facebook additionally noted that they publish information on "actions taken in response to government demands related to locally illegal content, including those related to alleged illegal misinformation," in its biannual Transparency Report.[292]

Twitter responded by referencing its Transparency Report and its legal request FAQ, which "details the approach we take, including a review of the reported account or Tweets for any indications that the request seeks to restrict or chill freedom of expression; raises other Twitter policy concerns (e.g., accounts belonging to journalists, verified accounts, or accounts containing political speech); or raises practical or technical concerns."[293]

PEN America is heartened that each technology company referenced its existing transparency reports in addressing our question. Certainly, first and foremost, social media companies must be as transparent as possible about these partnerships. While recognizing that information provided by law enforcement and intelligence agencies will not always be shareable with the public, as a rule, social media platforms must be as open as they can with users about what type of information they might share with government bodies and how they decide what to share and when. Platform users also need to inform themselves about the vast breadth of personal information collected on them, often in ways that are not obvious or visible. Despite the platforms' assurances of privacy, the existence and expansion of these government partnerships are a reminder that personal information may find its way into the hands of law enforcement. At the same time, platforms must ensure that they do not enable excessive government surveillance of users. The pressing nature of the threat does warrant information sharing; increased transparency around these processes is necessary to ensure the cure does not end up being more destructive than the disease.

Tech companies' collaborations with political campaigns can be even more questionable than their partnerships with government agencies. In the fall of 2017, a study published in the journal *Political Communication* detailed how Facebook, Google, and Twitter worked with campaigns during the 2016 election cycle. While the tech giants purported to be merely offering "customer support" to political campaigns that bought ads on their platforms—similar to services that they would offer any ad buyer—the study argued that they instead "actively shap[ed] campaign communication through their close collaboration with political staffers."[294] Daniel Kreiss, a professor at the University of North Carolina and one of the study's authors, deemed the active support "a form of subsidy from technology firms to political candidates."[295]

Soon afterward Brad Parscale, the Trump campaign's digital director, corroborated and advanced the study's findings, telling *60 Minutes* that Facebook staff were "embedded" inside Trump's offices.[296] Facebook disputed this designation while acknowledging that Facebook staff engaged with political campaigns , saying that "no one from Facebook was assigned full-time to the Trump campaign, or full-time to the Clinton campaign."[297] In response to a request for comment from PEN America, a Facebook spokesperson stated: "While particular candidates and campaigns may choose to make use of Facebook in different ways, we make the same level of support and resources available to all candidates and campaigns."[298] But the *Political Communication* study and *60 Minutes* report raise troubling questions about where tech companies should draw the line between giving campaigns customer support and actively working to support their candidates.

In response to request for comment from PEN America, a Twitter spokesperson stated: "we approach political clients in the same way we do commercial clients, offering support on how to use our tools and best practices for using Twitter. We do not embed employees in campaigns."[299] The platforms did not provide information on any specific assistance they had provided in 2018.

Technology companies may want to offer robust customer service to those who buy their ad space, but a political campaign is not just any customer. Major technology platforms already appear to be investigating how to collaborate with political campaigns to more effectively counter disinformation. But as they do so, they must be careful not to cross the line into advising these campaigns in ways that compromise their impartiality.

Government Response

The public's response to fraudulent news has included the expectation that government entities would act to tamp down on it as part of their obligation to ensure the integrity of our elections. This expectation has been shaken by the Trump Administration's reluctance to acknowledge Russia's interference in the 2016 elections, with the president himself repeatedly downplaying the Kremlin's disinformation incursions.[300] In the first 18 months of Trump's presidency, the White House reportedly held only two meetings on the subject of election security.[301]

On September 12, 2018, after significant pressure to take action, President Trump signed an executive order declaring that any attempts by foreign adversaries "to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of

election and campaign infrastructure or the covert distribution of propaganda and disinformation, constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States."[302] Although the order carefully avoids stating that interference has actually occurred, it threatens sanctions for anyone determined to have been involved in interfering in a U.S. election.[303]

On October 19, 2018, the Office of the Director of National Intelligence, the Department of Justice, the Department of Homeland Security, and the FBI issued a joint statement on combating foreign influence on U.S. elections.[304] The statement expressed concern about ongoing attempts by Russia, China, Iran, and others to "undermine confidence in democratic institutions and influence public sentiment and government policies."[305] The departments explicitly warned that such campaigns "may seek to influence voter perceptions and decision making in the 2018 and 2020 U.S. elections."[306] Also in October, NBC News reported on a DHS intelligence assessment that "Russia and China remain active, though in different ways. Russia attempts to spread disinformation with hackers posing as Americans, while China is engaged in more conventional propaganda efforts."[307] In a report to the White House 45 days after the 2018 election, as required in the executive order, the DNI confirmed that while it found no evidence of election infrastructure being compromised, "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests."[308] In December, then-Secretary of Defense James Mattis stated at a security forum in California that Russian President Vladimir Putin had "tried again to muck around in our elections last month."[309]

Despite the president's own insufficient response, federal departments and agencies have focused on various approaches to security election integrity.

In July 2018, NSA director and head of the Pentagon's U.S. Cyber Command, Paul Nakasone, established a Russia group to coordinate the efforts of the two organizations in countering influence operations related to the midterms.[310] The group was additionally directed to coordinate with the Department of Homeland Security, the CIA, and the FBI.[311]

The FBI is "the lead federal agency responsible for investigating foreign influence operations," which its website describes as including "fabricated stories on social media platforms to discredit U.S. individuals and institutions."[312] The website states that the FBI's Foreign Influence Task Force works to secure elections through investigations and operations; information and intelligence sharing with other intelligence community agencies, state and local law enforcement, and election officials; and private sector partnerships, namely "strategic engagement with U.S. technology companies, including threat indicator sharing."[313] In a statement at a press briefing on August 2, 2018, FBI Director Christopher Wray said that the bureau was providing tech companies with "actionable intelligence to better enable them to address abuse of their platforms by foreign actors. This year, we've met with top social media and technology companies several times. We've given them classified briefings, and we've shared specific threat indicators and account information, so they can better monitor their own platforms."[314]

In Colorado, on September 10, 2018, the FBI provided first-of-its-kind training for 150 state-level Colorado government officials, politicians, and campaign staff on cybersecurity and defending

against disinformation. The Colorado secretary of state, Wayne Williams, co-sponsored the event. Williams told *The Colorado Sun*: "My office will be monitoring and responding to things that appear to be providing misinformation or disinformation, but as a voter, check and make sure you know the source from which you are re-posting or re-tweeting. Check to make sure it actually is a fact before you share it with other people."[315] Mike Weissman, a Democratic state representative who attended the event, told PEN America that he found it worthwhile. "I'm sure they are going to be doing things like this every cycle," he said.[316] "By time we come to 2020, we will be talking about misinformation as regularly as who is going where in Iowa and New Hampshire."[317] PEN America reached out to the FBI to inquire if other such trainings had been held in 2018 or would be held in the future, but received no response.

In October 2018, *The New York Times* reported that the Pentagon's U.S. Cyber Command was targeting individual Russian operatives it believed were engaging in disinformation campaigns aimed at disrupting elections.[318] The *Times* called the effort "the first known overseas cyberoperation to protect American elections, including the November midterms."[319] The campaign involves telling individual Russian operatives that they are being tracked, as a deterrent measure. Jankowicz, of the Wilson Center, described this tactic as "messaging individual purveyors of disinformation, saying, in effect, 'We are watching you. We know what you are doing. If you continue, there might be consequences.'"[320]

On November 2, 2018, The Daily Beast reported that the United States was prepared for a possible cyberattack against Russia to retaliate for attempted electronic interference in the midterm elections and that military hackers had been given advance approval to access Russian systems in case the plan needed to be activated.[321] The report noted that "the effort constitutes one of the first major cyberbattle plans organized under a new government policy enabling potential offensive operations to proceed more quickly once the parameters have been worked out in advance and agreed among key agencies."[322]

On February 27, 2019 *The Washington Post* reported that U.S. Cyber Command had indeed taken action against the IRA on Election Day and approximately a day afterwards.[323] The report cited officials as saying the obstruction of the IRA's networks was intended to "prevent the Russians from mounting a disinformation campaign that cast doubt on the results."[324] While the move was hailed by lawmakers as having successfully defended against Russian election interference,[325] some officials were more realistic about the likely effect, with the *Post* quoting one as saying: "Causing consternation or throwing sand in the gears may raise the cost of engaging in nefarious activities, but it is not going to cause a nation state to just drop their election interference."[326] Others have suggested this action may have had unintended consequences within Russia. Russia-focused media startup The Bell noted that news of the attack might have been one factor behind the introduction of a bill intended to isolate Russia's internet, which was introduced in the state Duma a month after the election. The Bell called the attack "bad news for ordinary Russians," noting: "The idea to isolate the Russian internet appeared years ago, but the attack has surely given it a new urgency."[327]

On November 5, the day before the midterms, the DHS, DOJ, DNI, and FBI issued a joint statement warning Americans to be vigilant, stating that "foreign actors—and Russia in particular—continue to influence public sentiment and voter perceptions . . . by spreading false information about political processes and candidates, lying about their own interference

activities, disseminating propaganda on social media, and through other tactics."[328] Everyday Americans, these governmental bodies continued, "can mitigate these efforts by remaining informed, reporting suspicious activity, and being vigilant consumers of information."[329] The statement went on to urge citizens to get election information from state or local election officials and to verify that sources are reliable before sharing information on social media.[330] This statement can be read as an acknowledgment of the central conclusion of PEN America's 2017 report, *Faking News*, that perhaps the most powerful shield against foreign disinformation is not sophisticated cyber-tactics or classified intelligence sharing but citizens' thoughtful engagement with the news they consume.[331]

Upon leaving his post as Facebook's chief security officer in August 2018, Alex Stamos criticized the federal government for not doing enough to protect the election process from hacking and disinformation—specifically for failing in 2016 and not acting quickly enough to secure the 2018 midterms. "The fundamental flaws in the collective American reaction dates to summer 2016," Stamos wrote, "when much of the information being reported today was in the hands of the executive branch."[332] Now a professor at Stanford studying disinformation, Stamos added that in August, Facebook revealed details on scores of accounts Russians and Iranian groups that were used to distort information. "The revelations are evidence that Russia has not been deterred and that Iran is following in its footsteps," he wrote.[333] "This underlines a sobering reality: America's adversaries believe that it is still both safe and effective to attack U.S. democracy using American technologies and the freedoms we cherish."[334]

Stamos's point is valid. Like the tech companies, government is still playing catch-up in the wake of revelations about 2016, when it, too, was caught relatively flat-footed or failed to act on what it knew. After decades of the Cold War, in which propaganda campaigns between the United States and the Soviet Union were de rigueur, the U.S. government had clearly been lulled into a false sense of security with regard to those tactics.[335] A blog post on the legal analysis site Lawfare, in October 2017, noted that during the Cold War, disinformation campaigns rarely targeted the U.S. public, because Americans' reliance on a limited set of high-quality journalistic outlets made such efforts difficult.[336] But with the birth of the internet and significant changes across the information ecosystem, the public is now vulnerable in new ways. While the growing consensus that voluntary measures and algorithmic tweaks have fallen far short is heartening, it is clear that more comprehensive, thoughtful government action is needed to address these threats.

It is PEN America's position, however, that calls for greater government action must also be tempered with caution. In addition to the concerns raised previously regarding government collaboration with tech companies in ways that may infringe on free expression or user privacy, there are other risks involved. For one, as disinformation increasingly originates within the U.S., there may be a temptation to turn surveillance and cyberoperations typically used externally towards Americans. As such, the U.S. government response to threats from fraudulent news and disinformation needs to both match the scale of the problem and take care not to infringe on privacy and the right to free expression.

Political Parties

Both the Democratic National Committee and the Republican National Committee have stepped up their security, recognizing that they are vulnerable to foreign and domestic interference. Their focus, however, remains primarily on cybersecurity and the threat of hacking, perhaps in part due to the DNC's experience of having a raft of campaign emails published by Wikileaks after a successful Russian spearfishing attempt in 2016.[337] There appears to be little focus on fraudulent news and disinformation within the parties, either as a tool that might be used against campaigns and needs to be defended against, or as a strategy the party needs to ensure candidates and campaigns are not utilizing. A DNC memo sent out 100 days before the 2018 midterm elections and outlining various committee initiatives provided an update on cybersecurity but included no specific mention of plans to tackle disinformation campaigns.[338] Given the ways these tactics are used to discourage voter turnout or otherwise confuse voters, the parties certainly have an interest in developing strategies to address this challenge.

Raffi Krikorian, the DNC's chief technology officer, had a team of 35 people working on cybersecurity and disinformation.[339] Krikorian said that he "barely" interacted with his counterpart, the chief technology officer at the Republican National Committee, and that they communicate primarily via government agencies.[340] "Sadly, we don't work with them as closely as we would like," he said.[341] Although, as noted above, Twitter has described coordinating with both the RNC and DNC, they do not appear to have done much to coordinate with each other. With regard to tackling fraudulent information online, Krikorian has said that social media companies must do more as disinformation operations continue to grow: "Our concern is, honestly, it's just going to get worse over time unless the platform companies figure out how to control it on their side."[342] PEN America reached out to both the RNC and DNC for comment, but received no response.

The parties will need to start taking fraudulent news as seriously as they take cybersecurity, not only to reduce the risk of becoming targets but also to maintain their own credibility. The risk that fraudulent news will come to be viewed as an acceptable political tactic is real, and it will be up to candidates and parties to commit to upholding the truth and defending against the further erosion of our political discourse.

There is a fine line between purveying fraudulent news and aggressively micro-targeting voters with heavily partisan and negative campaign messages. A negative ad that in years past would have run on television or in print can take on vastly increased potency in the digital age, when it can be targeted, reinforced, and refined in real time to shape opinions in ways that are insidious and difficult to counter. Micro-targeting also means that many such ads are displayed to such a narrow slice of the public that the media, opposing campaigns, or public interest groups may never see them, much less have the opportunity to argue that they are false or misleading. In the wake of the 2016 elections and revelations about the rising technical sophistication of both legitimate and illegitimate election-related communications, candidates and parties are understandably seeking an edge from new, turbocharged forms of opinion shaping. In this context, it is essential that political organizations prioritize the obligation not to contribute to the degradation of election-related discourse by trafficking in misleading information.

Risks on the Horizon

The increasing ease with which people can produce, for example, "deepfake" videos—in which video imagery is digitally manipulated in ways that are extremely difficult to discern—could be exploited by purveyors of fraudulent news during the 2020 presidential elections. In May 2018, a political party in Belgium commissioned a fake video of Donald Trump offering advice to Belgium about climate change.[343] The party, Sp.a, assumed that the video edit was obvious enough that people would see that the video was a joke, intended to drive them to an online petition.[344] Many did not get the joke. Although some experts, including Tim Hwang, director of the Harvard-MIT Ethics and Governance of Artificial Intelligence Initiative, believe that the technology is not yet accessible enough to pose an imminent threat, the Belgium example shows that even crude fake videos can be convincing.[345] In the context of an election, a deepfake video—particularly if presented as news—could be nearly impossible to refute, its impact exceedingly difficult to mitigate. Danielle Citron, a law professor at the University of Maryland, told *The Guardian,* "I'm starting to see how a well-timed deep fake could very well disrupt the democratic process."[346] The very existence of deepfakes can erode public trust in even authentic video. As Hany Farid, professor of computer science at the University of California at Berkeley, put it: "The problem isn't just that deep fake technology is getting better. It is that the social processes by which we collectively come to know things and hold them to be true or untrue are under threat."[347]

Deepfakes are just the latest example of technology with the potential to erode our ability to assess the truth. While much of the fraudulent news that proliferated around the 2018 election was amateurish, it is the collective impact of fraudulent information that risks undermining fact-based civic dialogue. During elections, the impact is magnified, making it all the more urgent that we strengthen our societal resilience against such manipulation.

Fraudulent News in the 2018 Midterm Elections: What it Looked Like

Who Was Responsible: Foreign versus "Domesticated" Disinformation

After 2016, most media coverage of fraudulent news revolved around foreign actors: Russian agents of disinformation, along with Macedonian clickbait farmers, were seen as the primary antagonists, even as experts noted that ideologues here in the United States were also creating and disseminating fraudulent stories. As one report to the Senate Intelligence Committee said of the Russians, "The scale of their operation was unprecedented," representing a major offensive in a "propaganda war against American citizens."[348]

Two years and one midterm election cycle later, both the threat and our understanding of it have shifted. Foreign actors linked to Russia and Iran continued to use fraudulent news to stoke polarization and influence U.S. voters, with their activity seemingly less focused on specific

campaigns than in 2016. Part of this shift probably involves the nature of midterm elections; more local and more numerous, they are simply harder for outsiders to game, and they offer lower pay-offs in terms of influence and outcomes. And this does not mean influence efforts in 2020 will not be more explicitly about influencing election outcomes. Still, while foreign disinformation operations remain a major problem, in 2018 some significant fraudulent news attacks came from domestic actors.

During the month of October 2018, researchers from the Oxford Internet Institute examined some 2.5 million Tweets and nearly 7,000 Facebook pages to assess the spread of "junk news," which they defined as "deliberately misleading, deceptive, or incorrect information."[349] The researchers evaluated junk news purveyors on the basis of five criteria: professionalism, style, credibility, bias, and counterfeit. To qualify as a source of junk news, an outlet had to fulfill at least three of the five criteria.[350] So an outlet that was found to be heavily biased, to exhibit low levels of professionalism, and to assume a hyperbolic style could be considered junk news even if it was not deemed deliberately fraudulent. While that definition could therefore include sources that don't meet PEN America's criterion of intentional deception, the findings were nonetheless alarming.[351] The Oxford study concluded that the proportion of junk news circulating on social media was greater than during the 2016 election, with a five percent increase on Twitter, and that users shared more junk news than news from what the study defined as professional sources.[352] The biggest shift, though, represented a difference in kind rather than one of degree: "What we are seeing is home-grown conspiracy theories and falsehoods," said Lisa-Maria Neudert, one of the researchers. "The problem now reaches far beyond foreign influence campaigns and extremist fringe voices. Junk news has been domesticated, and social media users have an appetite."[353]

The Oxford researchers were not the only ones to reach this conclusion. On Election Day, *The Washington Post* described a "consensus among lawmakers, tech company officials and independent experts" that the new threat in disinformation is coming from within our borders.[354] In early October, *The New York Time*s reported that the website Right Wing News had used a coordinated network of Facebook pages and accounts to spread false stories about psychology professor Christine Blasey Ford to discredit her allegations of sexual misconduct against Brett Kavanaugh during his Supreme Court nomination hearings.[355] "There are now well-developed networks of Americans targeting other Americans with purposefully designed manipulations," commented Molly McKew, a researcher on information warfare.[356]

Graham Brookie, director and managing editor of the Atlantic Council's Digital Forensic Research Lab (@DFRLab), told PEN America that, while "misleading and polarizing disinformation from foreign actors targeting U.S. elections is still ongoing," the "scale and scope of misinformation and disinformation domestically is a lot larger than foreign actors working across elections. We are pretty good at driving disinformation at ourselves."[357]

Meanwhile, the disinformation threat from foreigners remains, and seems to be evolving. Recorded Future, a U.S.-based cybersecurity firm, found, and *The Wall Street Journal* reported, that the Russian social media accounts that it was tracking had changed tactics for the midterms, "from pushing verifiably false information to a greater emphasis on promoting 'hyperpartisan' perspectives."[358] Recorded Future suspected that Russian accounts were promoting narratives

from both ends of the political spectrum. Priscilla Moriuchi, the firm's director of strategic threat development, said that even in the two weeks leading up to the election, researchers had "seen tactics shift . . . to appear more real and legitimate."[359] On Election Day itself, she added, the accounts focused more heavily on allegations of voter fraud in the battleground states of Texas, Florida, and Ohio.[360]

During the 2018 cycle, Russian disinformation frequently appeared to have a broader aim than merely influencing congressional elections. While much domestic disinformation appears opportunistic and short-lived, Russian campaigns are playing a long game, stoking division and pushing more extreme political rhetoric with an eye toward weakening national cohesion and our democracy. Renée DiResta, director of research at New Knowledge, led one of the research teams behind the two December 2018 Senate reports that examined Russian interference in the 2016 election. In an opinion piece for *The New York Times* upon the report's release, DiResta stated that "Russia was able to masquerade successfully as a collection of American media entities, managing fake personas and developing communities of hundreds of thousands, building influence over a period of years and using it to manipulate and exploit existing political and societal divisions."[361]

In September 2018, the Department of Justice filed a 38-page criminal complaint against Elena Alekseevna Khusyaynova that described the Russian national as having managed the finances of "Project Lakhta," a Russian influence operation that targeted multiple countries, including the United States, over a period of several years.[362] The complaint states that, "since at least May 2014, Project Lakhta's stated goal in the United States was to spread distrust towards candidates for political office and the political system in general."[363] While the criminal complaint was backward looking, the Department made clear that Project Lakhta's activities were not confined to 2016 and instead stretched well onward into 2018.[364]

Members of Project Lakhta used thousands of fake Facebook accounts and email addresses to pose as Americans and engage in social media activity to "create and amplify divisive social and political content targeting a U.S. audience" and to promote or denigrate particular political candidates during both the 2016 and 2018 election cycles.[365] Contentious topics discussed in the group's social media posts included gun control, immigration, race, and LGBTQ rights. The project's social media activity did not reflect a single partisan preference, nor did it always come down on the same side of social issues, but it did, according to one participant, seek to "effectively aggravate the conflict between minorities and the rest of the population."[366]

The group's internal guidance, made public through the Department of Justice complaint, demonstrates that they understood and exploited Americans' different degrees of trust for various media outlets: "If you write posts in a liberal group . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed's titles."[367] On March 18, 2018, the project used a fake Twitter account, @wokeluisa, to post:

> Fun fact: the last time a new Republican president was elected without electoral fraud was in 1988[368]

On March 22, 2018, another fraudulent account associated with the project, @johncopper16, tweeted:

> Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your IA and 2A rights They hate the Police They hate the Military They hate YOUR President[369]

Perhaps most notably, the fraudulent accounts were already being used to post about the 2020 election, two and a half years away, as evidenced in a tweet from @johncopper16 on February 16, 2018, which also included a cheeky self-reference:

> Russians indicted today: 13 Illegal immigrants crossing Mexican border indicted today: 0 Anyway, I hope that all those Internet Research Agency f*ckers will be sent to gitmo.
>
> We didn't vote for Trump because of a couple of hashtags shilled by the Russians. We voted for Trump because he convinced us to vote for Trump. And we are ready to vote for Trump again in 2020![370]

In addition, the Kremlin is taking its divisive disinformation campaigns offline, too. As Renée DiResta told PEN America: "Rather than creating fake Facebook pages and growing their own communities from scratch, they are creating fake personas, then reaching out to real, existing activists who already have communities to coordinate protests. To attend protests. To photograph protests. To write content. To share their content."[371]

The New York Times covered another Russian attempt to stoke divisions in September 2018. A Russian-run website called USAReally (full name: "USA Really. Wake Up Americans") had launched in April and was, in the *Times*' words, "hiding in plain sight."[372] Its stated mission: "to promote crucial information and problems, which are hushed up by the conventional American media controlled by the establishment and oligarchy of the United States."[373]

The site, which has reportedly been banned by Facebook, Twitter, and Reddit for violating their terms of use,[374] mixes conspiracy theories and hyper-partisan stories with more legitimate news that is repackaged from more credible sources. Its Russian founder, Alexander Malkevich, has denied allegations that the site is a Russian influence operation, though he has acknowledged that it has received funding from Russian's state-connected Federal News Agency; the press release announcing USAReally's creation was published on that agency's website.[375]

The *Times* reported that several cybersecurity experts suspected that USAReally's transparent connections to Russia may be deliberate. In the words of private intelligence analyst Lee Foster, USAReally may be attempting to "move this type of activity more into the mainstream, to try to legitimize it as a media entity."[376] The goal, then, would be to promote Russian disinformation sites as simply another source of hyper-partisan news, another unsavory but permitted entrant into American's civic discourse. If this is true, then Russian disinformation agents may be seeking to accelerate exactly the trend that PEN America has feared: Americans simply resigning themselves to the further fragmentation of "truth" into shards of hyper-partisan and even fraudulent discourse.

At the same time, all propaganda should not be banned from social media—whether by the U.S. government or by technology giants following their own terms of service. Other Russian media organizations, such as the television news network RT (formerly Russia Today), are permitted on major social media platforms, as they should be. Voices that represent the views of other governments, even governments that can be hostile to American interests, form part of a diverse media landscape from which Americans can develop their opinions. Still, readers have a right to understand the sources of the news they consume and the ways those sources shape the news that is presented. For this reason, transparency around ownership is an important principle to uphold. Facebook's "context button," for example, appears on a news site's posts and links to its Wikipedia entry, theoretically providing a straightforward way for users to make their own decisions about what information to trust. The pop-up information for RT, for instance, says that it is a Russian news outlet funded by the Russian government.[377]

Russian agents' skill at fomenting division underscores the need for solutions that not only push back against fraudulent news but also encourage constructive conversations around ideological fault lines. Providing a foundation of credible, fact-based information to promote civil, enlightened discussions of our most contentious issues will ensure that Americans, not Russian trolls, set the terms of our national discourse.

Fraudulent News and Disinformation in the 2018 Election Cycle

Candidate Attacks

Predictably, a significant portion of fraudulent news in the 2018 midterm elections made false claims against individual candidates. These types of political lies are not new, but technology has allowed for far more sophisticated versions and for their vast and rapid spread.

For example, on October 7, 2018, a manipulated and inaccurately captioned photo of Stacey Abrams, the Democratic nominee for governor of Georgia, was posted on Facebook. The original photo showed Abrams standing with Linda Sarsour, a co-chair of the Women's March, both of them holding an Abrams campaign sign.[378] The photo was taken at a rally in January 2018 marking the march's one-year anniversary.[379] The doctored image added the word "Communist" and the hashtag "#MuslimBrotherhood" to the sign and was accompanied by text reading "Heads up Georgia. The Muslim Brotherhood is backing Abrams."[380] On October 8, 2018, FactCheck.org declared the photo doctored and noted that there was no evidence to support the claim of Abrams's association with the Muslim Brotherhood.[381] By then, thought, over 18,000 people had shared it.[382] Moreover, despite the fact that FactCheck.org reviewed the post as part of its partnership with Facebook to address fraudulent information, and despite the fact that the post was thoroughly debunked, it remains up on Facebook, available for sharing.

Photo credit: FactCheck.org

A meme falsely attributing a quote to Republican Senator Ted Cruz was first created by a satirical Facebook page in 2015 but was resurrected and spread in 2018 with no way for people to know that it had been intended as a parody.[383] The meme quotes Cruz saying: "When gays stayed hidden we had no mass shootings; we had no public nudity. Society was polite. Now anything and everything goes and I blame them."[384] PolitiFact reviewed the videotaped speech that supposedly contained those words, delivered by Cruz at the Conservative Political Action Committee (CPAC) conference in 2014, and found that it included no such quote.[385] The Facebook page where the meme first appeared—called "Stop the world: Teabaggers want to get off"—is now defunct, but according to PolitiFact, it originally described itself as "for entertainment purposes" and its content as "primarily satire and parody with a mix of political memes and messages."[386] The post demonstrates the difficulties of drawing a line between fraudulent news and satirical material that is spread with no connection to contextual information.

The disinformation campaigns did not end on Election Day. During her ultimately successful 2018 congressional campaign, Ilhan Omar, a Minnesota Democrat and Somali-American Muslim woman, was pilloried with fraudulent stories (including a claim that her ex-husband was actually her brother, whom she had married to get him American citizenship). One purveyor of this false news was a website called Stop Ilhan, which touts itself as "Prepared and paid for by the 5th Congressional District RPM, authorized by Jennifer Zielinski for Congress"; Zielinski was Omar's 2018 congressional opponent.[387] PEN America attempted to contact the MNGOP CD5, which purportedly paid for the site, for comment, as well as representatives of the Zielinski campaign to confirm if they had indeed authorized the website, but received no response.

After the election, Omar continued to be hounded by fraudulent news. Shortly after her victory, a meme was posted on Facebook with a *Time* magazine photo of her and a fake inflammatory quote that quickly went viral: "I think all white men should be put in chains as slaves because they will never submit to Islam."[388] In this case, the post was flagged and fact-checked by

PolitiFact as part of its recently launched partnership with Facebook,[389] and the original post was quickly removed from the platform,[390] an example—unlike the Stacey Abrams incident above—of a functioning fact-checking system.

SPOTLIGHT: DOMESTIC DISINFORMATION IN THE 2017 ALABAMA SENATE ELECTION

On December 19, 2018, *The New York Times* revealed that a group of Democratic tech experts had experimented with Russian-style online deceptions in the contentious 2017 Alabama Senate race between Republican Roy Moore—who had been accused of sexual misconduct with underage women—and the eventual winner, Democrat Doug Jones.[391] One part of the ruse attempted to divide Republican votes by creating a Facebook page that appeared to belong to conservative Alabamians and using it to endorse a Republican write-in candidate.[392] Another piece of this effort involved connecting seemingly Russia-linked Twitter accounts with Roy Moore's account. The sudden influx of ostensibly Russian accounts following Moore drew media coverage at the time, and Moore's campaign quickly pinned the blame on his Democratic opponent.[393] The Jones campaign denied the accusations, and no evidence of its involvement has surfaced.[394] An internal report on the operation, which was obtained by *The New York Times*, was unabashed in stating its tactics and intent: "We orchestrated an elaborate 'false flag' operation that planted the idea that the Moore campaign was amplified on social media by a Russian botnet."[395]

Among those *The New York Times* alleged were involved in the effort was Jonathon Morgan, the CEO of New Knowledge,[1] a cybersecurity firm that delivered a commissioned report to the Senate Intelligence Committee on Russian disinformation in the 2016 elections.[396] The Senate report is widely cited for its analysis and conclusions--including in this report. In a public statement published in January, Morgan stated that his and New Knowledge's involvement in online efforts around Alabama's special election was confined to a "small, limited research project on Facebook," to test "how liberals and conservatives responded to a variety of social media posts and memes" and to specifically determine "whether counter-messaging, delivered from credible news sources, such as *The Washington Post* and Fox News, could break through the information bubbles that surround Facebook users."[397]

The *Times* reported that the financing for the effort--reportedly $100,000--came from American Engagement Technologies (AET), an anti-disinformation company.[398] AET, in turn, was reportedly funded by Reid Hoffman, the co-founder of LinkedIn. Hoffman later apologized for his involvement, saying he was unaware that his money was being used to pay for such a disinformation effort and that he "categorically disavow[s] the use of misinformation to sway an election."[399] Morgan also expressed regret for his involvement with AET, and said, "I am angered by the way my work has been conflated with the claims in AET's report."[400] There is no evidence that Jones, his campaign, or party officials were aware of the effort, and he has called on the Federal Election Commission and the Department of Justice to investigate.[401]

[1] Elsewhere in this report, PEN America cites New Knowledge and its staff--not including Jonathon Morgan--in relation to their role as lead authors on one of the Senate reports on disinformation in the 2016 elections and as experts in Russian disinformation campaigns.

In the wake of the revelations, Facebook removed five accounts for engaging in coordinated inauthentic behavior, without identifying the individuals associated with them. Morgan, who confirmed that his account was among those shut down,[402] also acknowledged that he had created a fake Facebook page to mimic Russian disinformation tactics. He stated, however, that he created the fake page as "almost a thought experiment" to examine the ease of spreading fraudulent information, rather than with the goal of influencing the election.[403] The misinformation effort, Morgan argued, was "intended to help us understand how these kind of campaigns operated. We thought it was useful to work in the context of a real election but design it to have almost no impact."[404]

Regardless of precisely who was behind which parts of the effort, however, it is clear someone intended to affect the campaign and its outcome. According to *The New York Times*, internal documents from the Alabama disinformation project suggest that the intent was specifically to "enrage and energize Democrats" and "depress turnout" among Republicans. The documents boast, for instance, of "radicalizing Democrats with a Russian bot scandal."[405] They also make clear that the effort was modeled on "the tactics now understood to have influenced the 2016 elections."[406] Even accepting that some of those involved may have viewed the effort as a mere experiment, carrying out in such a test the midst of a live election raises obvious and serious ethical questions.

On January 7, 2019, the *Times* reported on a second project aimed at Moore in 2017. Revolving around a Facebook page titled Dry Alabama purported to be run by Baptist supporters of Moore, it advocated the prohibition of alcohol in the state. The page was operated by Democrats who wanted to see Moore defeated.[407] Its intention was apparently to exploit and intensify Republicans divisions between religious conservatives and business conservatives over restrictions on alcohol. One of those involved in the campaign said that its Facebook posts attracted 4.6 million views and 97,000 engagements.[408]

The *Washington Post* editorial board, commenting on the incident, concluded that a dangerous precedent had been set.[409] Part of the solution, it urged, was for "candidates, political committees, big nongovernmental organizations and others" to "pledge not to engage in inauthentic activity, just as the Democratic Congressional Campaign Committee promised not to promote hacked material in the 2018 midterms."[410]

Both operations demonstrate the risk that domestic actors will adopt tactics pioneered by foreign governments for manipulating elections and that such tactics may come to be seen as acceptable—even necessary—campaign tools. Matt Osborne, a progressive activist who participated in Dry Alabama, said that he thought deceptions like the one he engaged in should be banned, but in the meantime, "if you don't do it, you're fighting with one hand tied behind your back. You have a moral imperative to do this—to do whatever it takes."[411]

More broadly, the use of false flag tactics, as allegedly occurred in Alabama, risks further alienating Americans from the idea that there is any objective truth in politics whatsoever. Sowing such confusion makes it increasingly difficult for voters to distinguish true information from false, posing both a threat to the free expression right of individuals to access information, and to the integrity of our elections.

Blurred Boundaries: Disinformation, Satire, and Negative Ads

Before the election, several news outlets, including *The New York Times*, asked their audiences to send in examples of election-related misinformation. The *Times* received over 4,000 examples.[412] Among them were clear examples of disinformation, while others were less definitive. For instance, both Republicans and Democrats had created Facebook pages that attacked their candidates' opponents. The National Republican Senatorial Committee had produced pages including The Real Heidi Heitkamp, against the Democratic senator from North Dakota, who lost; Millionaire Claire, against the Democratic senator from Missouri, who also lost; and Radical Kyrsten, against the Democrat who ultimately won the Arizona Senate seat. The liberal PAC For our Future, meanwhile, created The Real Mike DeWine, against the successful Republican gubernatorial candidate for Ohio. While most of the accounts normally displayed a picture of the criticized candidates as their profile picture, a review of the content of the accounts made reasonably clear that they were intended as spoofs mounted by critics.

Each of these pages essentially functioned as a running series of attack ads, criticizing the candidate's record, positions, or qualifications. "Millionaire Claire," for example, featured a series of captioned photos and videos slamming Senator McCaskill for her purported opposition to tax reform and her purported personal wealth.[413] The *Times* pointed out that while such attack pages "don't technically violate Facebook's rules" as long as the sponsoring organization's name appears, such pages "can be confusing to the casual Facebook user scrolling through his or her feed."[414] The *Times* labeled the ads "potentially misleading."[415]

While PEN America agrees that these Facebook pages qualify as misleading, we do not consider them to be examples of fraudulent news. Social media accounts that depict themselves as a public figure *in a way that is clearly intended to be a critical and satirical representation of that person* do not attempt to deceive. There is a long tradition of political satire, in the form of comic sketches, cartoons, satirical writing, songs, and other types of content, that mocks public figures by impersonating them. Satire is a valued means of political expression, and the effort to crack down on deliberately misleading fraudulent news should avoid impinging upon it. In our previous report, we noted that satire does not constitute fraudulent news, even while acknowledging that a busy or distracted reader may mistakenly believe the satirical story to be real.

These impersonating Facebook pages may have triggered *Times* readers' negative responses in part because they constituted negative attacks, which are widely perceived as dirty politics and which often make misleading or out-of-context claims in their efforts to tarnish a candidate. But for an advertisement or other piece of content to cross the line from conventional, long-accepted attacks to the realm of fraudulent news hinges on several factors: (1) whether the claims made are accurate or false; (2) whether the source of the attack is transparent and verifiable; 3) whether the content is intentionally deceitful; and 4) whether a reasonable voter can grasp the intent and meaning of the content.

There is a valuable debate to be had over hardball negative campaign tactics. But that is a separate, albeit related, conversation from the one about fraudulent news. Both misleading attack ads and fraudulent news threaten to chip away at the edifice of truth that unifies our public discourse, and it is appropriate to demand more from our politics. And when an attack is patently and demonstrably false, it should indeed be called out as fraudulent. But, particularly when we ask technology companies and our government to "do something" about fraudulent news, we must keep our definitions clear and narrowly bounded in order to minimize the risk that this "something" will end up being an act of political censorship.

Political Moments and Fraudulent News

In a *New York Times* article summarizing the responses it received after calling on readers to share examples of election misinformation, tech reporter Kevin Roose described misinformation that "coalesces around major news events in what could be called 'hoax floods,' often adding to highly charged partisan conversations."[416] The two most prominent examples in this election cycle centered around the contentious confirmation hearings for Brett Kavanaugh, who faced allegations of sexual assault, and the so-called caravan of Central American migrants who were purportedly marching toward the U.S. border and became the subject of significant commentary from President Trump and conservative media.[417]

The *Times* devoted two separate articles to debunking "viral rumors" about Kavanaugh's accusers.[418] The rumors primarily focused on Professor Christine Blasey Ford, who testified at Kavanaugh's hearing that he had assaulted her when they were both in high school. The fraudulent information included attempts to link Blasey Ford and another accuser, Deborah Ramirez, to prominent philanthropist George Soros, bogeyman of countless conspiracy theories. A photo that circulated on social media claimed to show Ford with Soros but actually showed him with Ukrainian human rights activist Lyudmyla Kozlovska.[419]

Source: Twitter

An article published on the website Big League Politics claimed that Ramirez had received a fellowship from Soros's Open Society Foundations in 2013,[420] though it was a different woman by the same name who had received the fellowship.[421] The article was eventually deleted.[422] Another one, posted on the news site Grabien, claimed that Blasey Ford's students had rated her poorly on Rate My Professors but had confused her with a similarly named professor at a different university.[423] This article was picked up by the Drudge Report, re-posted under the all-caps headline "Christine Ford's Students Savage Her in Reviews,"[424] and shared on Facebook by Fox News host Laura Ingraham, who later deleted it. Grabien posted a correction and apology and retracted the article, which now appears with strikethrough text.[425] Several conservative news sites, including The Gateway Pundit, published a fraudulent claim that Kavanaugh's mother, herself a judge, had once ruled against Blasey Ford's parents in a foreclosure case, causing them to lose their house. Although CBS News and Snopes quickly proved that Judge Martha Kavanaugh's ruling had in fact allowed the Blaseys to keep their house,[426] the false claim remains on The Gateway Pundit, albeit with an update citing CBS News's findings.[427] The sloppiness and skirting of basic protocols of verification evidenced in these articles resulted in the irresponsible and damaging dissemination of falsehoods over a hot-button issue of the election cycle.

The fraudulent news about the so-called migrant caravan sought to send a message that a band of invaders posed an imminent danger to Americans. It was stoked by President Trump's frequent tweets, which had the clear intention of making the caravan a central election issue. CNN pointed out that, "from October 16 to November 6—aka Election Day—President Donald Trump sent 45 tweets mentioning the 'border' between the United States and Mexico."[428] But in the eight days following the election, he did not tweet once about the caravan and made only

a single reference to the border.[429] Perhaps Trump's most notorious claim came in an October 22 tweet in which he wrote, without evidence, that "unknown Middle Easterners" were part of the caravan.[430] This falsehood appears to have originated with remarks made earlier in October by Guatemalan President Jimmy Morales, who said that Guatemala had detained terrorists from the Islamic State on its territory and deported them to their country of origin (thereby making it impossible for them to be in the caravan).[431] Morales did not make a connection to the caravan; that idea seems to have come from Fox News's coverage of his remarks.[432] Days later, on October 25, the Republican Senate candidate in Maine, Eric Brakey, tweeted a baseless claim that Islamic State operatives in Central America were planning to infiltrate "refugee communities" to enter "western countries."[433]

On Facebook, a post shared thousands of times displayed photos that were said to depict bloodied Mexican police "being brutalized by members of this caravan."[434] The photographer later clarified on Facebook that the photos were taken in Mexico in 2012 during "a confrontation between students and police."[435]

Source: Twitter

Another conspiracy theory spread the baseless claim that George Soros was funding the caravan. A video, which showed members of the caravan receiving money, was tweeted by President Trump[436] and used to promote the Soros conspiracy theory.[437] Other posts suggested that support for the caravan was coming from the United Nations or from Democrats.[438]

In December 2018, Buzzfeed reported that fraudulent news may have actually birthed and expanded the caravan. An imposter Facebook account purporting to belong to a prominent Honduran activist and journalist spread false claims—primarily through Facebook Messenger—that well-known local groups were organizing a caravan (a not unprecedented act for migrants who sought safety in numbers).[439] The messages may have swelled the migrant contingent's ranks, which eventually grew to more than 7,000 people.[440]

These hoax floods underscore the way fraudulent news flourishes in an atmosphere of polarization—a phenomenon that agents of Russian disinformation appear to already understand and revel in, and that American social media users, including prominent politicians, are increasingly exploiting as well.

Voting and Election Day Disinformation

Fraudulent information is a problem that stretches well beyond the boundaries of any one particular election. However, perhaps the most dangerous form of fraudulent news are the fraudulent claims that directly relate to Election Day itself, eroding Americans' appreciation for the sanctity of the voting process and directly affecting our ability not only to make an informed voting decision, but to even know when, where, and how to vote.

On Election Day--which is after all a very specific window of time--fraudulent news featured or shared on social media is well-placed to outstrip the efforts of fact-checkers who might otherwise have more time to debunk fake stories. Twitter, in particular, is perhaps more likely to host disinformation on Election Day itself, given the platform's focus on immediate and bite-sized commentary. The Brennan Center for Justice, in its review of online voter suppression during the 2018 elections--with "voter suppression" referring to fraudulent news as well as other tactics designed to suppress voter turnout--declared that they found notable online suppression campaigns "especially" on Twitter.[441] In its Retrospective Review of the midterm elections, Twitter reported, "The vast majority of violative content we removed from our service on Election Day was voter suppressive content," amounting to 6,000 tweets.[442]

Below is a sampling of social media disinformation aimed at dampening turnout, spreading fear of nonexistent voter fraud, or stoking distrust in the voting process:

- Posts on Facebook stated that Immigration and Customs Enforcement (ICE) agents were patrolling the polls looking for undocumented citizens.[443] In apparent response to this disinformation, ICE tweeted once in October and again on Election Day: "ICE does not patrol or conduct enforcement operations at polling locations. Any flyers or advertisements claiming otherwise are false."[444] Facebook removed the posts.
- Twitter posts and Facebook posts listed the wrong date for Election Day. An analysis from the Brennan Center for Justice noted that incorrect Election Day information was a "very common" tactic within Twitter posts sharing fraudulent news, with some even helping to popularize the hashtag #votenovember7th . . . a strange example of a hashtag both promoting and itself containing fraudulent news, in less than 20 characters.[445]
- The Brennan Center also revealed that, while they did not find many examples of paid Facebook ads engaging in voter suppression, one paid ad that ran in Kansas--reportedly

sponsored by a Republican candidate for office and targeting women--falsely claimed that voters would need a birth certificate or naturalization document to register, even though the law that had supposedly put such a requirement in place had already been invalidated by the courts.[446]

- In North Dakota, where Democrat Heidi Heitkamp eventually lost her Senate seat to Republican Kevin Cramer, beginning five days before the election a Facebook ad appeared that said people risked losing out-of-state hunting licenses if they voted in North Dakota. While the ad was labeled as paid for by the North Dakota Democratic Party, it originated from a site with no obvious affiliation to the party. The North Dakota Democratic Party did not respond to a request for comment from Buzzfeed, which reported the story.[447] PEN America also attempted to contact the North Dakota Democratic Party, but received no response. The North Dakota Republican Party called the ad an effort at voter suppression.[448]

Source: Facebook (via Buzzfeed)[449]

- Multiple Facebook memes recirculated a years-old false claim that George Soros owns a company that makes voting machines.[450] The text of one post read: "ALERT: On Election Day if your voting machine is a SmartMatic brand request a paper ballot. SOROS owns SmartMatic brand. Under Fed Law u r entitled to a paper ballot. The following States have SmartMatic voting machines: AZ, CO, FL, VA, MI, NV, PA, CA, DC, IL, LA, MO, NJ, OR, WA, WI."[451] Another called for Soros to "remove his voting machines from all states."[452] The memes attracted anti-Semitic comments from users;[453] Soros is frequently the target of anti-Semitic conspiracy theories. The same falsehood was spread during the 2016[454] and 2012 election campaigns.[455] While not necessarily intended to sway the outcome of particular contests, such claims appear designed to undermine public trust in the integrity of the election.
- An Election Day tweet claimed to include video of voter fraud, with the text, "More voter fraud in Ohio. Why is it that all the errors are always the Democrats?? Because the only way they can win is if they cheat!! This madness needs to stop."[456] The video spread quickly, amassing 95,000 views.[457] It depicted a voting machine that appeared to be printing out results that did not match the voter's selection. The Franklin County Board of Elections issued a statement to clarify: "After reviewing the video and our Election

Day Issue Tracking software, we determined that particular machine had a paper jam and was taken off line. The voter in question was moved to another machine and cast their vote with no issues."[458] (The statement is no longer on the Franklin County website.) The user behind the original tweet shared the clarification as well.[459] Buzzfeed contacted Facebook, which had also posted the video and subsequently removed it from Facebook and Instagram. Despite notifications to Twitter, the video stayed on the site throughout Election Day.[460] Claire Wardle, a disinformation expert, explained that this was probably because the video itself was "true," meaning that it had not been doctored; it was the lack of context and the attached commentary claiming voter fraud were misleading. "It's the tactical part that should give them reason to take it down," Wardle said. "Twitter should think about the content that emerges on Election Day that tries to influence the vote."[461]

- Several viral Election Day tweets made false claims about undocumented immigrants voting. One used photos from a 2014 event to claim that citizens' militias at the U.S. border were detaining busloads of "illegals" who were "HEADED TO THE POLLS!!!"[462] Another falsely claimed that two busloads of "illegals" were stopped "with 'Beto' signs" and implied that they were being paid to vote.[463] That tweet was by Larry Schweikart, a retired history professor at the University of Dayton and coauthor of *A Patriot's History of the United States*.[464] "I'm only countering what goes on on the other side," Schweikart told Buzzfeed, adding that he wouldn't mind if the information was fake news. "*The New York Times* has yet to retract one in a billion articles so, no, it wouldn't bother me."[465]

When Buzzfeed asked Schweikart if he was concerned about spreading falsehoods, he said no: "Hey, fake news, right?" His contention that disinformation on one side justifies retaliatory disinformation from the other is a perspective that could easily become more common in the years ahead. This suggests a troubling future trajectory for political information wars where another party's alleged use of disinformation excuses one's own, and where fraudulent news becomes not an abhorrent lie but a morally justifiable tactic. Such rationalizations, it is easy to conclude, are further enabled by President Trump's condemnation of wide swathes of the media as "fake news," for no other reason than that he disagrees with their coverage. If a large segment of the American public believes that many of the most prestigious news outlets are actively disseminating disinformation, why shouldn't they be allowed to do the same?

This challenge underscores a fundamental truth about the way forward in addressing fraudulent news. Technical solutions from internet platforms can play a major role, and government action—tightly circumscribed by respect for the First Amendment—may also be warranted in certain areas. Ultimately, however, the work of fighting fraudulent news depends on restoring trust in our civic systems, working constructively to heal the painful divisions that others seek to exploit, encouraging media literacy, and renewing our shared commitment to the truth.

RECOMMENDATIONS

That politics and elections inspire participants to twist the truth is not news. But the migration of our political discourse from the realms and rhythms of television, print media, and snail mail

to the digital arena has given rise to new tools of opinion shaping that are fast evolving and hard to fully absorb. The 2016 election laid bare the potential for these new tools to exert stealthy and powerful influence on public opinion and, inevitably, voter behavior. The 2018 midterms showed how foreign actors are increasing their sophistication, and how these tools risk becoming more mainstream within domestic politics. And the coming years will inevitably be a period of trial and error as regulators, tech companies, parties, campaigns, and voters learn to navigate this new landscape.

As we look ahead to the presidential elections in 2020, it is clear that the scope and nature of the threat will both expand and evolve. The Director of National Intelligence's 2019 Worldwide Threat Assessment stated that "our adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests," and identified the use of disinformation, online influence operations, and deepfakes as among the key risks.[466] A report by Politico in February 2019 confirmed that such efforts are likely already underway, specifically targeting current or prospective Democratic presidential candidates with disinformation and misrepresentations of their views, and seemingly coordinated in a similar manner to attacks carried out by the Internet Research Agency in 2016.[467] Politico reported on analysis done by Guardians.ai, a tech company that fights information warfare, which found that the core set of accounts involved in spreading this information matched the accounts Guardians.ai had found had been active in spreading disinformation around voter fraud in 2018.[468] The Politico article also described the campaigns as "ill-equipped" to defend against these attacks.[469] The imperative for all campaigns and parties to take the threat of disinformation and influence operations seriously is clear, and urgent.

The danger that Americans' political views may be manipulated from without is real and alarming. But alongside it stands another, perhaps more insidious threat: that the architecture of our political system will collapse from within, a casualty of the erosion of truth and, ultimately, a widespread sense of resignation about the very existence of truth. Such a public posture is well-known in authoritarian settings, where media is distrusted and elections are widely regarded as illegitimate and meaningless. As the incidents documented in this report illustrate, there is already evidence that domestic political actors—whether individual politicians, parties, outside groups, or individuals—increasingly see deliberate, orchestrated disinformation as a necessary political tool. The notion that political actors have no choice but to fight fire with fire could lead to a deeply destructive spiral that debases our political discourse, making clear the urgency of taking action now.

In *Faking News*, PEN America's recommendations focused heavily on the role of news consumers, postulating that "measures to address the crisis of truth should first and foremost center on enabling and equipping people to derive, discern, and digest information in ways that gird against the influence of mendacious publication."[470] We continue to believe that empowered consumers of information are society's best defense against the scourge of fraudulent news and attempts to undermine the role of truth in our society. We are also cognizant that despite calls from us and others for the widespread implementation of news literacy curricula to inoculate a rising generation against false information, progress is slow and the issue has yet to win the broad recognition of urgency required to finance and mount such an effort. In the meantime, and probably beyond, tech giants, journalists, candidates, political parties, and legislators all have decisive roles to play in defending against fraudulent news. As

we look ahead to the 2020 elections, here are PEN America's recommendations to each of them.

We continue to believe that the spread of fraudulent news must not become a mandate for government or corporate censorship. At the same time, it is clear that many stakeholders feel both pressured and compelled to act, and that the public is looking to technology companies in particular to solve the problem. The actions taken by **technology companies** in the past year range from common sense policies that help consumers make more informed choices to aggressive, automated removals of accounts that have had an unintentional but nonetheless unacceptable censorious result. Tech companies may be taking action both as a response to user anger and as a way to preempt government regulation, but in doing so they face a dual risk of either implementing only cosmetic changes or overreaching in ways that restrict freedom of expression. A look at the breadth of solutions implemented by technology platforms to assess and respond to fraudulent information and political ads on the platforms suggests that, while both human and automated review are subject to bias, some combination of the two is likely the most reasonable approach. It is imperative that the companies that host such a vast portion of the political debate supplement their current tools with greater numbers of qualified, trained, and sufficiently supported personnel to evaluate content, exercise judgment, and adapt to fast-changing threats.

Foreign influence operations, particularly those that attempt to distort electoral outcomes, are a genuine concern of **government actors** and all Americans. But with little transparency about the growing coordination between government and technology companies and a host of outstanding questions about surveillance, privacy, and censorship, the role of law enforcement merits sustained and intensive scrutiny. Greater transparency is paramount.

PEN America remains wary of legislative solutions to fraudulent news, as the risk of content-based censorship and viewpoint discrimination is high. In particular, we continue to oppose legislative efforts to penalize online platforms for failing to remove certain types of fraudulent content. At the same time, **Congress** has a significant role to play. If crafted carefully, laws aimed at inducing companies to label advertising, conclusively verify the identities of significant customers, ferret out disinformation operations, and expand disclosure can restore and protect free expression. Congressional oversight, however, must be well-informed, and any legislative actions must be narrowly-bounded.

It is critical that credible **news media outlets** continue to uphold and exemplify the tenets of professional journalism, and they must work to make the process of professional journalism transparent to news consumers, lest their efforts to survive in the digital age end up hastening the devaluation of the currency of credible information. Around elections, efforts to catalog and fact check fraudulent news and disinformation are important and should continue, but should be carried out in real time so that voters have as much information as possible in advance of Election Day.

During elections, **individual candidates, political parties, and party committees** have a critical and fundamental role in protecting the integrity of our civic discourse and the public's ability to make informed decisions about who will represent them. Particularly as domestic disinformation becomes more common, political actors will have to make public and

unmistakable commitments to uphold the truth as part of their responsibility to the citizens they serve or seek to serve. PEN America endorses the proposal put forward by *The Washington Post*'s editorial board that candidates should pledge not to utilize fraudulent news as a political tactic,[471] and we believe that political parties and party committees should make the same commitment. We also recognize the work of Authentic Elections, a project started by media researcher Justin Hendrix, in sketching out several potential items to include in such a pledge, and we support the site's efforts to start a conversation about the need for a pledge through the hashtag #authenticelections.[472] Below, PEN America provides its own model pledge, intended as a starting point for such a commitment. We hope that candidates, parties, and party committees will commit to such a pledge as we enter the 2020 campaign season.

Fraudulent news, either homegrown or foreign, is just one piece of the larger challenge of an evolving ecosystem of how people receive and process news and information. For that reason, empowering **individual news consumers** to be informed and sophisticated in their ability to evaluate information remains the linchpin in the fight against fraudulent news. It was to this end that PEN America developed the News Consumers' Bill of Rights and Responsibilities, which was published with our *Faking News* report in 2017.[473] Empowering corporations or government as the leaders in solving this problem risks making them the arbiters of truth. Instead, that role must lie with the individual who will make the ultimate decision about what to believe or not believe, what to share or not to share. Multiple actors have a role to play in creating the enabling environment for individuals to understand the risks and how to defend against them, but especially in the context of elections, it is the individual voter who will ultimately decide what political tactics become acceptable, and which are rejected.

As we look ahead to the 2020 elections, no participant in the political ecosystem can avoid being on notice that fraudulent news and information represent a serious risk. Technology companies that have until now been experimenting with tools and methods now need to synthesize what they have learned to prevent their platforms from continuing to enable the subversion of American democracy. They must overcome their propensity to over-rely on automated solutions, recognizing their clear limitations and augmenting such efforts with a force of trained individuals who can apply human judgment—genuine rather than artificial intelligence—to make the difficult, real-time decisions necessary to counter fraudulent information while minimizing infringements on free speech.

<u>For Policy Makers, Civil Society, Social Media Platforms, and News Outlets:</u>

- Recognize, describe, and treat fraudulent news as an ongoing threat to the health of our civic discourse and democratic system, no matter its source.
- Stand in defense of professional news media and freedom of the press.
- Oppose government efforts that would impinge on free expression by requiring platforms to act as the ultimate arbiters of truth.
- Educate news consumers and voters on their rights and responsibilities and how to access credible election-related information.[474]

<u>For Policy Makers:</u>

The president and executive branch officials should:

- Establish that countering fraudulent efforts to influence U.S. elections is a matter of national security.
- Foster coordination across government agencies to share information and strategies to address foreign election influence operations and other election-related fraud.
- Press tech companies to provide adequate resources for efforts to counter election-related disinformation.

Legislators should:

- Establish a federal, bipartisan, independent, high-ranking commission to research, analyze, and propose solutions to help combat the spread of disinformation.
-
- Avoid broad legislation that overregulates online content or compels technology companies to adjudicate what is true and what is false.
- Support narrowly tailored legislative requirements for the disclosure of online political advertising sources and for transparency in how ads are targeted.
- Support state and local efforts to combat the spread of election- and candidate-related disinformation and help respond to local cybersecurity concerns leading up to Election Day.

Law enforcement and intelligence agencies must:

- Ensure that their efforts to safeguard electoral integrity and defend against fraudulent news and influence operations—including through coordination with technology companies—do not infringe on the free expression rights of individuals.

<u>For Social Media Platforms</u>

- In preparation for the 2020 election, immediately recruit and employ substantial teams of lawyers, advertising experts, linguists, graphics experts and election experts in numbers sufficient to materially augment still-developing and experimental AI and algorithmic approaches, bringing a trained, expert human eye to content, taking proactive approaches and making discerning judgments between legitimate expression and fraudulent information.
- Ensure that efforts to counter fraudulent content adhere to a narrow definition of "demonstrably false information that is being presented as fact in an effort to deceive the public."
- Increase transparency in decision making, including rulings about the removal of content or accounts.
- Ensure that all content moderation is conducted with adherence to clear community standards and carried out in a manner that respects and upholds users' rights.
- Ensure that appeal mechanisms are clear and accessible, involve the independent review of initial decision making, and include access to readily contactable, trained human interlocutors available on hotlines to answer election-related questions and deal with issues as they arise.
- Ensure that efforts to increase political ad transparency do not infringe on protected political speech.

- Increase transparency in coordination with law enforcement and intelligence agencies, making clear to users what types of information may be shared and under what conditions.
- Uphold user privacy policies when coordinating or information-sharing with government agencies.
- Continue efforts to improve coordination with academics and researchers so that all relevant stakeholders can better understand the spread of fraudulent news on social media platforms, the way it is weaponized during elections, and its effect on the public.
- Provide frequent public updates on new challenges and platform policies concerning fraudulent news and false information.
- Continue and expand support for professional journalism.
- End programs to embed staff in political campaigns as technical advisers, to avoid conflicts of interest and ensure that coordination with campaigns is focused on safeguarding information and users.

For News and Media Outlets:

- Continue to rigorously investigate and write about the harms posed by the spread of fraudulent news, to hold perpetrators responsible, and to examine and investigate the actions taken by technology companies in response.
- Continue to document and debunk fraudulent news regularly and particularly in the context of electoral campaigns.
- Prioritize making news-gathering operations more transparent for consumers, including finding new ways to educate readers about how professional journalism is done.
- Particularly in the context of elections, clearly label different types of content as reporting, commentary, opinion, analysis, etc., ensuring that such labels travel with content as it is posted and shared across the internet.

For Candidates and Political Parties:

- Refrain from deploying fraudulent news as a political tactic and from encouraging affiliated groups to participate in disinformation campaigns.
- Unequivocally denounce the use of fraudulent news by others, including supporters and members of your party, and including when it is used against political opponents.
- Encourage campaigns and party organs to commit to rejecting fraudulent news and disinformation tactics.
- Adopt, and endorse, a public document formalizing the commitment to these principles (see Appendix I for PEN America's proposed Model Pledge).

APPENDIX I: PEN AMERICA MODEL PLEDGE AGAINST FRAUDULENT NEWS

As public servants, figures placed in a position of authority in American politics, and aspirants to positions of public trust, we recognize our solemn duty to the American people to promote and uphold the highest standards of public service in our party's candidates. This duty includes a respect for the truth. The American people deserve leaders who are committed to the value of truth in our public discourse, regardless of political affiliation or ideology.

Fraudulent news—demonstrably false information that is being presented as fact in an effort to deceive the public—is harmful to our democracy. We denounce fraudulent news as contrary to the values of our republic and disrespectful to our citizens, who rely on factual information to make reasoned decisions. We recognize that fraudulent news is illegitimate and abhorrent, and must never become an acceptable political tactic.

Accordingly, we publicly pledge:

1. *To refrain* from creating, disseminating, promoting, or encouraging fraudulent news. In situations where we have mistakenly shared or promoted news that we later learn to be fraudulent, we will acknowledge our mistake and make a prominent public statement that such news is false.
2. *To insist* that our party's candidates for public office make similar commitments.
3. *To denounce* fraudulent news—including when it is directed at a political opponent or promoting a political cause that we support.
4. *To reject* the support of those who deliberately create or disseminate fraudulent news, regardless of their role in our causes or campaigns.
5. *To refuse* to endorse any candidate for public office who has disseminated fraudulent news or has refused to condemn fraudulent news disseminated by any organization supporting their candidacy.

---

[1] Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *The New York Times*, Sept. 20, 2018, nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html

[2] "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," Office of the Director of National Intelligence, Jan. 6, 2017, dni.gov/files/documents/ICA_2017_01.pdf

[3] See: Philip N. Howard, et al., "The IRA, Social Media and Political Polarization in the United States, 2012-2018," Computational Propaganda Project, comprop.oii.ox.ac.uk/research/ira-political-polarization/; Renee DiResta, et al., "The Tactics & Tropes of the Internet Research Agency," New Knowledge, cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf; Craig Timberg and Tony Romm, "New report on Russian disinformation, prepared for the Senate, shows the operation's scale and sweep," *The Washington Post,* December 17, 2018, washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/?utm_term=.cf797f14d09a; Scott Shane and Sheera Frankel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media," *The New York Times*, December 17, 2018, nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html

[4] "SSCI Research Summary," New Knowledge, Dec. 1, 2018, disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Slides.pdf

[5] Tara McGowan , panelist, "Social Media and the 2018 Campaign," Bipartisan Policy Center, filmed Sept. 20, 2018 at the Bipartisan Policy Center, Washington, DC, bipartisanpolicy.org/events/social-media-in-the-2018-campaign/
[6] Charlie Warzel, "There Was No Midterm Misinformation Crisis Because We've Democratized Propaganda," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/charliewarzel/midterms-fake-news-apocalypse-facebook-twitter
[7] Charlie Warzel, "There Was No Midterm Misinformation Crisis Because We've Democratized Propaganda," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/charliewarzel/midterms-fake-news-apocalypse-facebook-twitter
[8] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[9] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[10] Claire PEN Wardle, interview by PEN America, Dec. 1, 2018 (email)
[11] Claire PEN Wardle, interview by PEN America, Dec. 1, 2018 (email)
[12] Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[13] According to a report by the Knight Foundation called "Trust, Media and Democracy Initiative," "Seventy-three percent of Americans say that the spread of inaccurate information on the internet is a major problem with news coverage today, more than any other potential type of news bias. Just 50 percent of them feel confident that people can cut through bias to sort out the facts in the news—down from 66 percent a generation ago. And less than one-third of Americans say that they, personally, are very confident that they can tell when a news source is reporting factual news versus commentary or opinion." See Knight Foundation, "10 Reasons Why American Trust in the Media is at an All-Time Low," Medium, Jan. 16, 2018, medium.com/trust-media-and-democracy/10-reasons-why-americans-dont-trust-the-media-d0630c125b9e
[14] Emily Stewart, "2018's record-setting voter turnout, in one chart," *Vox*, Nov. 19, 2018, vox.com/policy-and-politics/2018/11/19/18103110/2018-midterm-elections-turnout
[15] "PEN International Charter," PEN International, accessed Jan. 30, 2019, pen-international.org/who-we-are/the-pen-charter
[16] Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[17] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html?emc=edit_ne_20181011&nl=evening-briefing&nlid=38046571201810 11&te=1
[18] Katerina Eva Matsa and Elisa Shearer, "News Use Across Social Media Platforms 2018," Pew Research Center, Sept. 10, 2018, journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/
[19] Katerina Eva Matsa and Elisa Shearer, "News Use Across Social Media Platforms 2018," Pew Research Center, Sept. 10, 2018, journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/
[20] Elisa Shearer and Jeffrey Gottfried, "News Use Across Social Media Platforms 2017," Pew Research Center, Sept. 7, 2017, journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/
[21] Katerina Eva Matsa and Elisa Shearer, "News Use Across Social Media Platforms 2018," Pew Research Center, Sept. 10, 2018, journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/
[22] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[23] *See e.g.* Sebastian Huempfer, "How Facebook's algorithm change is affecting publishers," *Medium*, April 26, 2018, medium.com/echobox/how-facebooks-algorithm-change-is-affecting-publishers-96cfc1ff4ed
[24] See: Cecilia Kang, Nicholas Fandos and Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times*, Oct. 31, 2017, nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html; "Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy," *The New York Times*, April 10, 2018, nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html; Adi Roberston and Casey Newton, "The 7 biggest moments from Wednesday's social media hearings," *The Verge*, Sept. 5, 2018, theverge.com/2018/9/5/17823280/facebook-twitter-hearings-congress-jack-dorsey-sheryl-sandberg; Katy Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing With Facebook and Twitter Execs," *Time*, Sept. 5, 2018, time.com/5387560/senate-intelligence-hearing-facebook-twitter/
[25] Evelyn Douek, "Senate Hearing on Social Media and Foreign Influence Operations: Progress, But There's A Long Way to Go," *Lawfare*, Sept. 6, 2018, lawfareblog.com/senate-hearing-social-media-and-foreign-influence-operations-progress-theres-long-way-go; Evelyn Douek, "Transatlantic Techlash Continues as U.K. and U.S. Lawmakers Release Proposals for Regulation," *Lawfare*, Aug. 8, 2018, lawfareblog.com/transatlantic-techlash-continues-uk-and-us-lawmakers-release-proposals-regulation; Katy Steinmetz, "Lawmakers Hint at Regulating Social Media During Hearing With Facebook and Twitter Execs," *Time*, Sept. 5, 2018, time.com/5387560/senate-intelligence-hearing-facebook-twitter/

[26] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian*, March 17, 2018, theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[27] Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg and Jack Nicas, "Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis," *The New York Times*, Nov. 14, 2018, nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html?action=click&module=inline&pgtype=Homepage
[28] Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants," *The New York Times*, Dec. 18, 2018, nytimes.com/2018/12/18/technology/facebook-privacy.html
[29] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[30] Kurt Wagner, "Mark Zuckerberg says it's 'crazy' to think fake news stories got Donald Trump elected," *Recode*, Nov. 11, 2016, recode.net/2016/11/11/13596792/facebook-fake-news-mark-zuckerberg-donald-trump; "Number of monthly active Facebook users worldwide as of 4th quarter 2018 (in millions)," Statista, 2019, statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[31] Jen Weedon, William Nuland and Alex Stamos, "Information Operations and Facebook," Facebook, April 27, 2017, fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf; Mark Zuckerberg, "I just went live a minute ago. Here's what I said," Facebook, Sept. 21, 2017, facebook.com/zuck/posts/10104052907253171; *see also* Scott Shane and Mike Isaac, "Facebook to Turn Over Russian-Linked Ads to Congress," *The New York Times*, Sept. 21, 2017, nytimes.com/2017/09/21/technology/facebook-russian-ads.html
[32] Alex Stamos, An Update On Information Operations On Facebook," Facebook Newsroom, Sept. 6, 2017, newsroom.fb.com/news/2017/09/information-operations-update/
[33] Alex Stamos, An Update On Information Operations On Facebook," Facebook Newsroom, Sept. 6, 2017, newsroom.fb.com/news/2017/09/information-operations-update/
[34] Alex Stamos, An Update On Information Operations On Facebook," Facebook Newsroom, Sept. 6, 2017, newsroom.fb.com/news/2017/09/information-operations-update/
[35] Mark Zuckerberg, "Preparing for Elections," Facebook Note, Sept. 12, 2018, facebook.com/notes/mark-zuckerberg/preparing-for-elections/10156300047606634/
[36] https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html
[37] "Removing Bad Actors on Facebook," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[38] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[39] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[40] Nicholas Fandos, Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts," The New York Times, July 31, 2018, nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html
[41] Rob Price, "Facebook built an election 'war room' to try to avoid repeating the mistakes of 2016—here's what it's like inside," *Business Insider*, Oct. 18, 2018, businessinsider.com/inside-facebook-election-war-room-2018-10
[42] Kurt Wagner and Rani Molla, "Facebook has disabled almost 1.3 billion fake accounts over the past six months," *Recode*, May 15, 2018, recode.net/2018/5/15/17349790/facebook-mark-zuckerberg-fake-accounts-content-policy-update
[43] "How are ads related to politics and national issues identified on Facebook?," Facebook Help Center, accessed Jan. 30, 2019, facebook.com/help/180607332665293?helpref=faq_content&utm_source=The%20Sift&utm_campaign=5674912387-The%20Sift%20Sept.%2029%202017_COPY_01&utm_medium=email&utm_term=0_5cfd351768-5674912387-182560049
[44] "Ad Archive," Facebook, accessed Jan. 31, 2019, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=f525457687&e=5cb5c6a55f
[45] Tessa Lyons, "Hard Questions: What's Facebook's Strategy for Stopping False News?," Facebook Newsroom, May 23, 2018, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=3f13c10d1c&e=5cb5c6a55f
[46] David Ingram, "Facebook opens up to researchers—but not about 2016 election," *NBC News*, Aug. 18, 2018, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=c7f7327b80&e=5cb5c6a55f
[47] Taylor Hughes, Jeff Smith and Alex Leavitt, "Helping People Better Assess the Stories They See in News Feed with the Context Button," Facebook Newsroom, April 3, 2018, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=806aa27dda&e=5cb5c6a55f

[48] Dan Zigmond, "Machine Learning, Fact-Checkers and the Fight Against False News," Facebook Newsroom, April 8, 2018, newsroom.fb.com/news/2018/04/inside-feed-misinformation-zigmond/
[49] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[50] "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[51] Adam Mosseri, "News Feed Ranking in Three Minutes Flat," Facebook Newsroom, May 22, 2018, newsroom.fb.com/news/2018/05/inside-feed-news-feed-ranking/
[52] Adam Mosseri, "Addressing Hoaxes and Fake News," Facebook Newsroom, Dec. 15, 2016, newsroom.fb.com/news/2016/12/news-feed-fyi-addressing-hoaxes-and-fake-news/
[53] Tessa Lyons, "Hard Questions: What's Facebook's Strategy for Stopping False News?," Facebook Newsroom, June 14, 2018, newsroom.fb.com/news/2018/06/hard-questions-fact-checking/; "Third-Party Fact-Checking on Facebook," Facebook Business, accessed Jan. 31, 2019, facebook.com/help/publisher/182222309230722
[54] Alex Peysakhovich and Kristin Hendrix, "Further Reducing Clickbait in Feed," Facebook Newsroom, Aug. 4, 2016, newsroom.fb.com/news/2016/08/news-feed-fyi-further-reducing-clickbait-in-feed/; Dan Zigmond, "Machine Learning, Fact-Checkers and the Fight Against False News," Facebook Newsroom, April 8, 2018, newsroom.fb.com/news/2018/04/inside-feed-misinformation-zigmond/
[55] PEN America interview with Katie Harbath, Sept. 13, 2018 (phone)
[56] PEN America interview with Katie Harbath, Sept. 13, 2018 (phone)
[57] PEN America interview with Katie Harbath, Sept. 13, 2018 (phone)
[58] Daniel Funke, "Facebook is now downranking stories with false headlines," *Poynter*, Oct. 24, 2018, poynter.org/fact-checking/2018/facebook-is-now-downranking-stories-with-false-headlines/?utm_source=Daily+Lab+email+list&utm_campaign=9550b37655-dailylabemail3&utm_medium=email&utm_term=0_d68264fd5e-9550b37655-364612713
[59] Daniel Funke, "Facebook is now downranking stories with false headlines," *Poynter*, Oct. 24, 2018, poynter.org/fact-checking/2018/facebook-is-now-downranking-stories-with-false-headlines/?utm_source=Daily+Lab+email+list&utm_campaign=9550b37655-dailylabemail3&utm_medium=email&utm_term=0_d68264fd5e-9550b37655-364612713
[60] Daniel Funke, "Facebook is now downranking stories with false headlines," *Poynter*, Oct. 24, 2018, poynter.org/fact-checking/2018/facebook-is-now-downranking-stories-with-false-headlines/?utm_source=Daily+Lab+email+list&utm_campaign=9550b37655-dailylabemail3&utm_medium=email&utm_term=0_d68264fd5e-9550b37655-364612713
[61] Holmes Lybrand, "Kavanaugh 'Stated He'd Overturn' *Roe V. Wade*?," *The Weekly Standard*, Sept. 10, 2018, weeklystandard.com/holmes-lybrand/fact-check-has-brett-kavanaugh-stated-hed-overturn-roe-v-wade; Daniel Funke, "The Weekly Standard Fact Check vs. ThinkProgress, explained," *Poynter*, Sept. 13, 2018, poynter.org/fact-checking/2018/the-weekly-standard-fact-check-vs-thinkprogress-explained/
[62] Ian Millhiser, "Brett Kavanaugh said he would kill Roe v. Wade last week and almost no one noticed," *ThinkProgress*, Sept. 9, 2018, thinkprogress.org/brett-kavanaugh-said-he-would-kill-roe-v-wade-last-week-and-almost-no-one-noticed-c0e98494b06d/
[63] Daniel Funke, "The Weekly Standard Fact Check vs. ThinkProgress, explained," *Poynter*, Sept. 13, 2018, poynter.org/fact-checking/2018/the-weekly-standard-fact-check-vs-thinkprogress-explained/
[64] Joseph Menn, "Exclusive: Facebook to ban misinformation on voting in upcoming U.S. elections," *Reuters*, Oct. 15, 2018, reuters.com/article/us-facebook-election-exclusive/exclusive-facebook-to-ban-misinformation-on-voting-in-upcoming-u-s-elections-idUSKCN1MP2G9
[65] Tessa Lyons, "Hard Questions: What's Facebook's Strategy for Stopping False News?," Facebook Newsroom, June 14, 2018, newsroom.fb.com/news/2018/06/hard-questions-fact-checking/; see also: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[66] Tessa Lyons, "Hard Questions: What's Facebook's Strategy for Stopping False News?," Facebook Newsroom, June 14, 2018, newsroom.fb.com/news/2018/06/hard-questions-fact-checking/
[67] Vinny Green and David Mikkelson, "A Message to Our Community Regarding the Facebook Fact-Checking Partnership," Snopes, Feb. 1, 2019, snopes.com/snopes-fb-partnership-ends/
[68] Vinny Green and David Mikkelson, "A Message to Our Community Regarding the Facebook Fact-Checking Partnership," Snopes, Feb. 1, 2019, snopes.com/snopes-fb-partnership-ends/
[69] Daniel Funke, "Snopes pulls out of its fact-checking partnership with Facebook," *Poynter*, Feb. 1, 2019, poynter.org/fact-checking/2019/snopes-pulls-out-of-its-fact-checking-partnership-with-facebook/
[70] Daniel Funke, "Snopes pulls out of its fact-checking partnership with Facebook," *Poynter*, Feb. 1, 2019, poynter.org/fact-checking/2019/snopes-pulls-out-of-its-fact-checking-partnership-with-facebook/
[71] Sam Levin, "Snopes quits Facebook's factchecking program amid questions over its impact," *The Guardian*, Feb. 1, 2019, theguardian.com/technology/2019/feb/01/snopes-facebook-factchecking-program-false-news

[72] "Community Standards Enforcement Report," Facebook, accessed Feb. 24, 2019, transparency.facebook.com/community-standards-enforcement#fake-accounts
[73] John Shinal, "Facebook shuts down 1 million accounts per day but can't stop all 'threat actors,' security chief says," *CNBC*, Aug. 24, 2017, cnbc.com/2017/08/24/facebook-removes-1-million-accounts-every-day-security-chief-says.html
[74] John Shinal, "Facebook shuts down 1 million accounts per day but can't stop all 'threat actors,' security chief says," *CNBC*, Aug. 24, 2017, cnbc.com/2017/08/24/facebook-removes-1-million-accounts-every-day-security-chief-says.html
[75] John Shinal, "Facebook shuts down 1 million accounts per day but can't stop all 'threat actors,' security chief says," *CNBC*, Aug. 24, 2017, cnbc.com/2017/08/24/facebook-removes-1-million-accounts-every-day-security-chief-says.html
[76] See: "The Santa Clara Principles on Transparency and Accountability in Content Moderation," accessed Jan. 31, 2019, santaclaraprinciples.org/
[77] "The Santa Clara Principles on Transparency and Accountability in Content Moderation," accessed Jan. 31, 2019, santaclaraprinciples.org/
[78] "An Open Letter to Mark Zuckerberg," Nov. 13, 2018, santaclaraprinciples.org/open-letter/#response
[79] "Facebook's Response," accessed Jan. 31, 2019, santaclaraprinciples.org/open-letter/#response
[80] Facebook spokesperson, interviewed by PEN America, February 11, 2019 (phone and email)
[81] Nick Clegg, "Charting a Course for an Oversight Board for Content Decisions," Facebook Newsroom, Jan. 28, 2019, newsroom.fb.com/news/2019/01/oversight-board/
[82] "Draft Charter: An Oversight Board for Content Decisions," Facebook Newsroom, Jan. 28. 2019, fbnewsroomus.files.wordpress.com/2019/01/draft-charter-oversight-board-for-content-decisions-1.pdf
[83] Nick Clegg, "Charting a Course for an Oversight Board for Content Decisions," Facebook Newsroom, Jan. 28, 2019, newsroom.fb.com/news/2019/01/oversight-board/; see also: Evelyn Douek, "Facebook's 'Draft Charter' for Content Moderation: Vague, But Promising," *Lawfare*, Jan. 31, 2019, lawfareblog.com/facebooks-draft-charter-content-moderation-vague-promising for analysis
[84] Facebook spokesperson, interviewed by PEN America, February 11, 2019 (phone and email)
[85] Nathaniel Gleicher, "Coordinated Inauthentic Behavior Explained," Facebook Newsroom, Dec. 6, 2018, newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/ (see video)
[86] Nathaniel Gleicher, "Coordinated Inauthentic Behavior Explained," Facebook Newsroom, Dec. 6, 2018, newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/ (see video)
[87] Nathaniel Gleicher and Oscar Rodriguez, "Removing Additional Inauthentic Activity from Facebook," Facebook Newsroom, Oct. 11, 2018, newsroom.fb.com/news/2018/10/removing-inauthentic-activity/
[88] Nathaniel Gleicher and Oscar Rodriguez, "Removing Additional Inauthentic Activity from Facebook," Facebook Newsroom, Oct. 11, 2018, newsroom.fb.com/news/2018/10/removing-inauthentic-activity/
[89] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[90] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[91] Nathaniel Gleicher and Oscar Rodriguez, "Removing Additional Inauthentic Activity from Facebook," Facebook Newsroom, Oct. 11, 2018, newsroom.fb.com/news/2018/10/removing-inauthentic-activity/
[92] Nathaniel Gleicher, "Election Update," Facebook Newsroom, Nov. 5, 2018, newsroom.fb.com/news/2018/11/election-update/
[93] Sheera Frenkel and Mike Isaac, "Russian Trolls Were at It Again Before Midterms, Facebook Says," *The New York Times*, Nov. 7, 2018, nytimes.com/2018/11/07/technology/facebook-russia-midterms.html?
[94] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[95] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[96] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[97] See: Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[98] Nathaniel Gleicher and Oscar Rodriguez, "Removing Additional Inauthentic Activity from Facebook," Facebook Newsroom, Oct. 11, 2018, newsroom.fb.com/news/2018/10/removing-inauthentic-activity/
[99] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[100] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html

[101] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[102] Nicholas Fandos and Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts," *The New York Times*, July 31, 2018, nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html
[103] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[104] Nathaniel Gleicher, "What We've Found So Far," Facebook Newsroom, July 31, 2018, newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/
[105] Nicholas Fandos and Kevin Roose, "Facebook Identifies an Active Political Influence Campaign Using Fake Accounts," *The New York Times*, July 31 2018, nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html
[106] The Shut It Down D.C. Coalition, Pastebin, accessed Feb. 1, 2019, pastebin.com/raw/p9zFffHi
[107] Dan Tynan, "Facebook accused of censorship after hundreds of US political pages purged," *The Guardian*, Oct. 16, 2018, theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship
[108] Dan Tynan, "Facebook accused of censorship after hundreds of US political pages purged," *The Guardian*, Oct. 16, 2018, theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship
[109] Dan Tynan, "Facebook accused of censorship after hundreds of US political pages purged," *The Guardian*, Oct. 16, 2018, theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship
[110] Marc Belisle, "Everything I Wrote Was True And Accurate. So Why Did Facebook Purge My Work?," *Buzzfeed News*, Oct. 17, 2018, buzzfeednews.com/article/marcbelisle/why-did-facebook-purge-reverb-press
[111] @JamesReader_RP, October 12, 2018. The original tweet has since been removed (as James Reader's account has been suspended by Twitter), but the Tweet to which he was responding, from Buzzfeed Media Editor, remains available at https://twitter.com/CraigSilverman/status/1050809834059309057
[112] "Reverb Press," Media Bias Fact Check, last modified July 2, 2018, mediabiasfactcheck.com/reverb-press/
[113] Craig Silverman (@CraigSilverman), "The removals are part of the company's stepped-up efforts ahead of the midterms and its work to combat misinformation overall," Twitter, Oct. 11, 2018, twitter.com/CraigSilverman/status/1050447031347474432
[114] Dan Tynan, "Facebook accused of censorship after hundreds of US political pages purged," *The Guardian*, Oct. 16 2018, theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship
[115] Dan Tynan, "Facebook accused of censorship after hundreds of US political pages purged," *The Guardian*, Oct. 16 2018, theguardian.com/technology/2018/oct/16/facebook-political-activism-pages-inauthentic-behavior-censorship
[116] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[117] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[118] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[119] Nina Jankowicz, interview by PEN America, October 25, 2018 (in person)
[120] Josh Constine, "Facebook denies report that election war room was disbanded," *TechCrunch*, Dec. 2018, techcrunch.com/2018/11/26/facebook-war-room-rages-on/
[121] Rob Price "Facebook built an election 'war room' to try to avoid repeating the mistakes of 2016—here's what it's like inside," *Business Insider*, Oct. 18, businessinsider.com/inside-facebook-election-war-room-2018-10
[122] "Q&A on Upcoming US and Brazil Elections," Facebook Newsroom, Sept. 19, 2018, newsroom.fb.com/news/2018/09/us-brazil-elections/
[123] Sarah Frier, "Facebook's Sheryl Sandberg Is Tainted by Crisis After Crisis," *Bloomberg*, Nov. 26, 2018, bloomberg.com/news/articles/2018-11-26/facebook-s-sheryl-sandberg-is-tainted-by-crisis-after-crisis; Sheera Frenkel and Mike Isaac, "Russian Trolls Were at It Again Before Midterms, Facebook Says," *The New York Times*, Nov. 7, 2018, nytimes.com/2018/11/07/technology/facebook-russia-midterms.html
[124] Sheera Frenkel and Mike Isaac, "Russian Trolls Were at It Again Before Midterms, Facebook Says," *The New York Times*, Nov. 7, 2018, nytimes.com/2018/11/07/technology/facebook-russia-midterms.html
[125] Hunt Allcott, Matthew Gentzkow and Chuan Yu, "Trends in the Diffusion of Misinformation on Social Media," Stanford Institute for Economic Policy Research, Oct. 2018, web.stanford.edu/~gentzkow/research/fake-news-trends.pdf
[126] Hunt Allcott, Matthew Gentzkow and Chuan Yu, "Trends in the Diffusion of Misinformation on Social Media," Stanford Institute for Economic Policy Research, Oct. 2018, web.stanford.edu/~gentzkow/research/fake-news-trends.pdf

[127] Hunt Allcott, Matthew Gentzkow and Chuan Yu, "Trends in the Diffusion of Misinformation on Social Media," Oct. 2018, web.stanford.edu/~gentzkow/research/fake-news-trends.pdf
[128] Tessa Lyons, "New Research Shows Facebook Making Strides Against False News," Facebook Newsroom, Oct. 19, 2018, newsroom.fb.com/news/2018/10/inside-feed-michigan-lemonde/
[129] Andrew Guess et al., "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 U.S. midterm election campaign," Feb. 15, 2019, personal.umich.edu/~bnyhan/fake-news-2018.pdf
[130] Andrew Guess et al., "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 U.S. midterm election campaign," Feb. 15, 2019, personal.umich.edu/~bnyhan/fake-news-2018.pdf (page 2)
[131] Andrew Guess et al., "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 U.S. midterm election campaign," Feb. 15, 2019, personal.umich.edu/~bnyhan/fake-news-2018.pdf (page 21)
[132] Andrew Guess et al., "Fake news, Facebook ads, and misperceptions: Assessing information quality in the 2018 U.S. midterm election campaign," Feb. 15, 2019, personal.umich.edu/~bnyhan/fake-news-2018.pdf (page 14)
[133] Craig Silverman and Scott Pham, "These are 50 Of The Biggest Fake News Hits On Facebook In 2018," *Buzzfeed News*, Dec. 28, 2018, buzzfeednews.com/article/craigsilverman/facebook-fake-news-hits-2018
[134] Craig Silverman and Scott Pham, "These are 50 Of The Biggest Fake News Hits On Facebook In 2018," *Buzzfeed News*, Dec. 28, 2018, buzzfeednews.com/article/craigsilverman/facebook-fake-news-hits-2018; see also: Craig Silverman, "Publishers Are Switching Domain Names To Try And Stay Ahead Of Facebook's Algorithm Changes," *Buzzfeed News*, March 1, 2018, buzzfeednews.com/article/craigsilverman/publishers-are-switching-domain-names-to-try-and-stay-ahead
[135] Jonathan Albright, "The Shadow Organizing of Facebook Groups," *Medium*, Nov. 4, 2018, medium.com/s/the-micro-propaganda-machine/the-2018-facebook-midterms-part-ii-shadow-organization-c97de1c54c65
[136] Jonathan Albright, "The Shadow Organizing of Facebook Groups," *Medium*, Nov. 4, 2018, medium.com/s/the-micro-propaganda-machine/the-2018-facebook-midterms-part-ii-shadow-organization-c97de1c54c65
[137] Jonathan Albright, "The Shadow Organizing of Facebook Groups," *Medium*, Nov. 4, 2018, medium.com/s/the-micro-propaganda-machine/the-2018-facebook-midterms-part-ii-shadow-organization-c97de1c54c65
138 Cameron Hickey, interview with PEN America, March 7, 2019 (by email)
[139] "Number of monthly active Twitter users worldwide from 1st quarter 2010 to 3rd quarter 2018 (in millions)," Statista, accessed Feb. 24, 2019, statista.com/statistics/282087/number-of-monthly-active-twitter-users/
[140] "Number of monthly active Twitter users in the United States from 1st quarter 2010 to 3rd quarter 2018 (in millions," Statista, accessed Feb. 24, 2019, statista.com/statistics/274564/monthly-active-twitter-users-in-the-united-states/
[141] Matthew Hindman & Vlad Barash, "DISINFORMATION, 'FAKE NEWS' AND INFLUENCE CAMPAIGNS ON TWITTER," Knight Foundation, Oct. 4, 2018, https://www.knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter
[142] Id.
[143] "Study: Twitter bots played disproportionate role spreading misinformation during 2016 election," News at IU Bloomington, Nov. 20, 2018, news.iu.edu/stories/2018/11/iub/releases/20-twitter-bots-election-misinformation.html
[144] "Study: Twitter bots played disproportionate role spreading misinformation during 2016 election," News at IU Bloomington, Nov. 20, 2018, news.iu.edu/stories/2018/11/iub/releases/20-twitter-bots-election-misinformation.html; Chengcheng Shao et al., "The spread of low-credibility content by social bots," *Nature Communications* 9, no. 1 (Nov. 20, 2018): 4787, doi.org/10.1038/s41467-018-06930-7
[145] Nir Grinberg et al., "Fake news on Twitter during the 2016 U.S. presidential election," *Science* 363, no. 6425 (Jan. 25, 2019): 374-378, doi.org/10.1126/science.aau2706
[146] Brian Heater, "Jack Dorsey admits Twitter hasn't 'figured out' approach to fake news," *TechCrunch*, Aug. 2018, techcrunch.com/2018/08/19/jack-dorsey-admits-twitter-hasnt-figured-out-approach-to-fake-news/ (see video)
[147] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, 52, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[148] Twitter Public Policy, "Update: Russian interference in the 2016 US presidential election," Twitter Blog, Sept. 28, 2017, blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html
[149] Twitter Public Policy, "Update: Russian interference in the 2016 US presidential election," Twitter Blog, Sept. 28, 2017, blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html
[150] "The Twitter Rules," Twitter Help Center, accessed Feb. 4, 2019, help.twitter.com/en/rules-and-policies/twitter-rules
[151] "The Twitter Rules," Twitter Help Center, accessed Feb. 4, 2019, help.twitter.com/en/rules-and-policies/twitter-rules

[152] Yoel Roth and Del Harvey, "How Twitter is fighting spam and malicious automation," Twitter Blog, June 26, 2018, blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html
[153] Del Harvey and Yoel Roth, "An update on our elections integrity work," Twitter Blog, Oct. 1, 2018, blog.twitter.com/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html
[154] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[155] "The Twitter Rules," Twitter Help Center, accessed Feb. 4, 2019, help.twitter.com/en/rules-and-policies/twitter-rules
[156] Yoel Roth and Del Harvey, "How Twitter is fighting spam and malicious automation," Twitter Blog, June 26, 2018, blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html
[157] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[158] Vijaya Gadde and Yoel Roth, "Enabling further research of information operations on Twitter," Twitter Blog, Oct. 17, 2018, blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html; Yoel Roth, "Empowering further research of potential information operations," Twitter Blog, Jan. 31, 2019, blog.twitter.com/en_us/topics/company/2019/further_research_information_operations.html
[159] Craig Timberg and Elizabeth Dwoskin, "Twitter is sweeping out fake accounts like never before, putting user growth at risk," *The Washington Post*, July 6, 2018, washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.01742acbeb16; "Number of monthly active Twitter users worldwide from 1st quarter 2010 to 3rd quarter 2018 (in millions)," Statista, statista.com/statistics/282087/number-of-monthly-active-twitter-users/
[160] Craig Timberg and Elizabeth Dwoskin, "Twitter is sweeping out fake accounts like never before, putting user growth at risk," *The Washington Post*, July 6, 2018, washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.01742acbeb16
[161] Nina Jankowicz, interview by PEN America, Oct. 25, 2018 (in person)
[162] Nina Jankowicz, interview by PEN America, Oct. 25, 2018 (in person)
[163] Del Harvey and Yoel Roth, "An update on our elections integrity work," Twitter Blog, Oct. 1, 2018 blog.twitter.com/official/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html
[164] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[165] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[166] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[167] Del Harvey and Yoel Roth, "An update on our elections integrity work," Twitter Blog, Oct. 1, 2018, blog.twitter.com/official/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html; see also: Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[168] Del Harvey and Yoel Roth, "An update on our elections integrity work," Twitter Blog, Oct. 1, 2018, blog.twitter.com/official/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html
[169] Christopher Bing, "Exclusive: Twitter deletes over 10,000 accounts that sought to discourage U.S. voting," *Reuters*, Nov. 2, 2018, reuters.com/article/us-usa-election-twitter-exclusive/exclusive-twitter-deletes-over-10000-accounts-that-sought-to-discourage-u-s-voting-idUSKCN1N72FA
[170] Donie O'Sullivan, "Twitter took down thousands of accounts that discouraged voting in midterms," *CNN*, Nov. 3, 2018, cnn.com/2018/11/02/tech/twitter-accounts-discourage-voting/index.html; Christopher Bing, "Exclusive: Twitter deletes over 10,000 accounts that sought to discourage U.S. voting," *Reuters*, Nov. 2, 2018, reuters.com/article/us-usa-election-twitter-exclusive/exclusive-twitter-deletes-over-10000-accounts-that-sought-to-discourage-u-s-voting-idUSKCN1N72FA
[171] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[172] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[173] Bridget Coyne, "Introducing US Election Labels for Midterm Candidates," Twitter Blog, May 23, 2018, blog.twitter.com/official/en_us/topics/company/2018/introducing-us-election-labels-for-midterm-candidates.html
[174] Bridget Coyne, "Introducing US Election Labels for Midterm Candidates," Twitter Blog, May 23, 2018, blog.twitter.com/official/en_us/topics/company/2018/introducing-us-election-labels-for-midterm-candidates.html
[175] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf.
[176] "US elections," Twitter, accessed Feb. 25, 2019, twitter.com/i/events/960990507714330625

[177] Charlie Warzel and Ryan Mac, "Twitter Just Launched A Midterm Elections Page And It's Already Full of Garbage," *Buzzfeed News*, Oct. 30, 2018, buzzfeednews.com/article/charliewarzel/twitter-just-launched-a-midterms-page-and-its-already
[178] Charlie Warzel and Ryan Mac, "Twitter Just Launched A Midterm Elections Page And It's Already Full of Garbage," *Buzzfeed News*, Oct. 30, 2018, buzzfeednews.com/article/charliewarzel/twitter-just-launched-a-midterms-page-and-its-already
[179] Charlie Warzel and Ryan Mac, "Twitter Just Launched A Midterm Elections Page And It's Already Full of Garbage," *Buzzfeed News*, Oct. 30, 2018, buzzfeednews.com/article/charliewarzel/twitter-just-launched-a-midterms-page-and-its-already
[180] Charlie Warzel and Ryan Mac, "Twitter Just Launched A Midterm Elections Page And It's Already Full of Garbage," *Buzzfeed News*, Oct. 30, 2018, buzzfeednews.com/article/charliewarzel/twitter-just-launched-a-midterms-page-and-its-already
[181] "US elections," Twitter, accessed Feb. 25, 2019, twitter.com/i/events/960990507714330625
[182] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf
[183] Daniel Funke and Alexios Mantzarlis, "Here's what to expect from fact-checking in 2019," *Poynter*, Dec. 18, 2018, poynter.org/fact-checking/2018/heres-what-to-expect-from-fact-checking-in-2019/
[184] Nahema Marchal et al., "Polarization, Partisanship and Junk News Consumption on Social Media During the 2018 US Midterm Elections," Oxford University, Nov. 1, 2018, blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2018/11/marchal_et_al.pdf; "Junk news dominating coverage of US midterms on social media, new research finds," University of Oxford News & Events, Nov. 1, 2018, ox.ac.uk/news/2018-11-01-junk-news-dominating-coverage-us-midterms-social-media-new-research-finds; Kate Conger and Adam Satariano, "Twitter Says It Is Ready for the Midterms, but Rogue Accounts Aren't Letting Up," *The New York Times*, Nov. 5, 2018, nytimes.com/2018/11/05/technology/twitter-fake-news-midterm-elections.html
[185] Nahema Marchal et al., "Polarization, Partisanship and Junk News Consumption on Social Media During the 2018 US Midterm Elections," Oxford University, Nov. 1, 2018, blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2018/11/marchal_et_al.pdf; Kate Conger and Adam Satariano, "Twitter Says It Is Ready for the Midterms, but Rogue Accounts Aren't Letting Up," *The New York Times*, Nov. 5, 2018, nytimes.com/2018/11/05/technology/twitter-fake-news-midterm-elections.html
[186] Kate Conger and Adam Satariano, "Twitter Says It Is Ready for the Midterms, but Rogue Accounts Aren't Letting Up," *The New York Times*, Nov. 5, 2018, nytimes.com/2018/11/05/technology/twitter-fake-news-midterm-elections.html
[187] Joe Perticone, "The Senate is tearing into Google for refusing to send a top exec to testify -- and even left an empty chair and name tag to highlight its displeasure," *Business Insider*, Sept. 5, 2018, businessinsider.com/us-senate-tears-into-google-for-refusing-to-send-top-executive-to-testify-2018-9
[188] Joe Perticone, "The Senate is tearing into Google for refusing to send a top exec to testify -- and even left an empty chair and name tag to highlight its displeasure," *Business Insider*, Sept. 5, 2018, businessinsider.com/us-senate-tears-into-google-for-refusing-to-send-top-executive-to-testify-2018-9
[189] Alexis C. Madrigal, "What Google's CEO Couldn't Explain to Congress," *Medium*, Dec. 12, 2018, medium.com/the-atlantic/what-googles-ceo-couldn-t-explain-to-congress-fed97ef4d6f0&sa=D&ust=1546454111508000&usg=AFQjCNFEZc8206FUQisRZ8WFTCu7faRS8g
[190] Mathew Ingram, "Why did Youtube stay with Google instead of going with Alphabet?," *Fortune*, Aug. 11, 2015, fortune.com/2015/08/11/youtube-google-alphabet/
[191] Written Testimony of Richard Salgado, Hearing on "Extremist Content and Russian Information Online: Working with Tech to Find Solutions", Senate Judiciary Subcommittee on Crime and Terrorism, Oct. 31, 2017, judiciary.senate.gov/imo/media/doc/10-31-17%20Salgado%20Testimony.pdf
[192] Craig Timberg, Drew Harwell and Tony Romm, "YouTube excels at recommending videos -- but not at detecting hoaxes," *The Washington Post*, Feb. 22, 2018, washingtonpost.com/business/technology/youtube-excels-at-recommending-videos—but-not-at-detecting-hoaxes/2018/02/22/6063268e-1803-11e8-92c9-376b4fe57ff7_story.html?utm_term=.ebe2bcc0027c; Alex Hern, "YouTube to crack down on fake news, backing 'authoritative' sources," *The Guardian*, July 9, 2018, theguardian.com/technology/2018/jul/09/youtube-fake-news-changes
[193] Barbara Ortutay, "YouTube is cracking down on 'fake news' with new text previews," *USA Today*, July 9, 2018, usatoday.com/story/tech/2018/07/09/youtube-cracks-down-fake-news/769861002/
[194] Elizabeth Dwoskin, "YouTube is changing its algorithms to stop recommending conspiracies," *The Washington Post*, Jan. 25, 2019, washingtonpost.com/technology/2019/01/25/youtube-is-changing-its-algorithms-stop-recommending-conspiracies/?utm_term=.521ce7a00116
[195] Alexios Mantzarlis, "Google is now highlighting fact checks in search," *Poynter*, April 7, 2017, poynter.org/news/google-now-highlighting-fact-checks-search

[196] "See Fact Checks in Search Results," Google Search Help, Google, accessed Feb. 25, 2019, support.google.com/websearch/answer/7315336?hl=en
[197] "What does each label mean?," Publisher Center Help, Google, accessed Feb. 25, 2019, support.google.com/news/publisher-center/answer/4582731?hl=en#fact-checking
[198] Alexios Mantzarlis, "Google is now highlighting fact checks in search," *Poynter*, April 7, 2017, poynter.org/news/google-now-highlighting-fact-checks-search
[199] Daniel Funke and Alexios Mantzarlis, "Here's what to expect from fact-checking in 2019," *Poynter*, Dec. 18, 2018, poynter.org/fact-checking/2018/heres-what-to-expect-from-fact-checking-in-2019/
[200] Michael Bertini, "How Google Is Addressing Fake News," *EContent*, Oct. 29, 2018, econtentmag.com/Articles/Editorial/Industry-Insights/How-Google-Is-Addressing-Fake-News-128238.htm
[201] "Learn about a news publisher," Google Search Help, Google, accessed Feb. 25, 2019, support.google.com/websearch/answer/7568277?hl=en
[202] Rhett Jones, "Why Google's Half-Assed Fact-Checking Widget Was Destined to Piss Off Conservatives," Gizmodo, Jan. 16, 2018, gizmodo.com/why-googles-half-assed-fact-checking-widget-was-destine-1822005133
[203] Daniel Funke, "Google suspends fact-checking feature over quality concerns," *Poynter*, Jan. 19, 2018, poynter.org/fact-checking/2018/google-suspends-fact-checking-feature-over-quality-concerns/
[204] "Learn about a news publisher," Google Search Help, Google, accessed Feb. 25, 2019, support.google.com/websearch/answer/7568277?hl=en
[205] Daniel Funke, "Google is building a search engine for fact checks," *Poynter*, Oct. 2, 2018, poynter.org/fact-checking/2018/google-is-building-a-search-engine-for-fact-checks/; "Fact Check Tools," Google, accessed Feb. 25, 2019, toolbox.google.com/factcheck/
[206] Kent Walker, "An update on state-sponsored activity," Safety and Security, Google, Aug. 23, 2018, blog.google/technology/safety-security/update-state-sponsored-activity/
[207] Kent Walker, "An update on state-sponsored activity," Safety and Security, Google, Aug. 23, 2018, blog.google/technology/safety-security/update-state-sponsored-activity/
[208] Kent Walker, "An update on state-sponsored activity," Safety and Security, Google, Aug. 23, 2018, blog.google/technology/safety-security/update-state-sponsored-activity/
[209] Google News Initiative, Google, accessed Feb. 25, 2019, newsinitiative.withgoogle.com/
[210] Richard Gingras, "Elevating quality journalism on the open web," Google News Initiative, Google, March 20, 2018, blog.google/outreach-initiatives/google-news-initiative/elevating-quality-journalism/
[211] Google News Initiative, Google, accessed Feb. 25, 2019, newsinitiative.withgoogle.com/
[212] Kevin Roose, "Google Pledges $300 Million to Clean Up False News," *The New York Times*, March 20, 2018, nytimes.com/2018/03/20/business/media/google-false-news.html
[213] Simon Rogers, "How Google is helping local journalists report on the midterm elections," Google News Initiative, Google, Sept. 19, 2018, blog.google/outreach-initiatives/google-news-initiative/how-google-helping-local-journalists-report-midterm-elections/
[214] Simon Rogers, "How Google is helping local journalists report on the midterm elections," Google News Initiative, Google, Sept. 19, 2018, blog.google/outreach-initiatives/google-news-initiative/how-google-helping-local-journalists-report-midterm-elections/
[215] Simon Rogers, "How Google is helping local journalists report on the midterm elections," Google News Initiative, Google, Sept. 19, 2018, blog.google/outreach-initiatives/google-news-initiative/how-google-helping-local-journalists-report-midterm-elections/; Derek Willis, Gabrielle LaMarr LeMee and Matthew Gerring, "Election Databot," *ProPublica*, last modified Nov. 10, 2018, projects.propublica.org/electionbot/
[216] David Dieudonné, "CrossCheck: Partnering with First Draft and newsrooms in the leadup to French elections," Google in Europe, Google, Feb. 6, 2017, blog.google/around-the-globe/google-europe/crosscheck-first-draft-newsrooms-french-elections/; The Trust Project, 2017, thetrustproject.org/
[217] Tiffany Hsu, "Voter Suppression and Racial Targeting: In Facebook's and Twitter's Words," *The New York Times*, Dec. 17, 2018, nytimes.com/2018/12/17/business/russia-voter-suppression-facebook-twitter.html; Daisuke Wakabayashi, "Google Finds Accounts Connected to Russia Bought Election Ads," *The New York Times*, Oct. 9, 2017, nytimes.com/2017/10/09/technology/google-russian-ads.html
[218] Alex Stamos, "An Update On Information Operations On Facebook," Facebook Newsroom, Sept. 6, 2017, newsroom.fb.com/news/2017/09/information-operations-update/
[219] Scott Shane and Mike Isaac, "Facebook to Turn Over Russian-Linked Ads to Congress," *The New York Times*, Sept. 21, 2017, nytimes.com/2017/09/21/technology/facebook-russian-ads.html
[220] Renee DiResta, et al., "The Tactics & Tropes of the Internet Research Agency," New Knowledge, int.nyt.com/data/documenthelper/533-read-report-internet-research-agency/7871ea6d5b7bedafbf19/optimized/full.pdf#page=1

[221] Natasha Singer, "'Weaponized Ad Technology': Facebook's Moneymaker Gets a Critical Eye," *The New York Times*, Aug. 16, 2018, nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html?module=inline
[222] Honest Ads Act, S. 1989, 115th Congress (2017-2018)
[223] Mark Zuckerberg, "With important elections coming up in the US, Mexico, Brazil, India, Pakistan, and more countries in the next year," Facebook, April 6, 2018, facebook.com/zuck/posts/10104784125525891; Twitter Public Policy (@Policy), "Twitter is moving forward on our commitment to providing transparency for online ads," Twitter, April 10, 2018, twitter.com/Policy/status/983734920383270912?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E983734920383270912&ref_url=https%3A%2F%2Ftechcrunch.com%2F2018%2F04%2F10%2Ftwitter-honest-ads-act%2F
[224] Denise Clifton, "Why Facebook and Twitter Aren't Stopping the Flood of False and Toxic Content," *Mother Jones*, Dec. 4, 2018, motherjones.com/media/2018/12/facebook-twitter-fake-news-toxic-content-social-media-companies/
[225] Google spokesperson, interviewed by PEN America, February 13, 2019 (email)
[226] Facebook spokesperson, interviewed by PEN America, February 11, 2019 (phone and email)
[227] Twitter Spokesperson, interviewed by PEN America, February 25, 2019 (email)
[228] Each platform uses their own definition for political advertisements. More information on these definitions can be found at the following links: https://business.twitter.com/en/help/ads-policies/restricted-content-policies/political-campaigning.html; https://support.google.com/adspolicy/answer/6014595#700 & https://support.google.com/adspolicy/answer/143465#533; https://www.facebook.com/business/help/1838453822893854?ref=fbb_blog.
[229] Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?," *The New York Times*, Sept. 2, 2018, nytimes.com/2018/09/02/technology/03adarchive.html
[230] "The Authorization Process for US Advertisers to Run Political Ads on Facebook is Now Open," Facebook Business, April 23, 2018, facebook.com/business/news/the-authorization-process-for-us-advertisers-to-run-political-ads-on-facebook-is-now-open; "About verification for election advertising and political affiliation in personalized advertising in the United States," Advertising Policies Help, Google, accessed Feb. 25, 2019, support.google.com/adspolicy/answer/9002729?hl%3Den&sa=D&ust=1546454111614000&usg=AFQjCNEIa6vDM5bZ5slloyHj1_N39V_-fQ; Vijaya Gadde and Bruce Falck, "Increasing Transparency for Political Campaigning Ads on Twitter," Twitter Blog, May 24, 2018, blog.twitter.com/official/en_us/topics/company/2018/Increasing-Transparency-for-Political-Campaigning-Ads-on-Twitter.html
[231] Del Harvey and Bruce Falck, "Announcing new US issue ads policy," Twitter Blog, Aug. 30, 2018, blog.twitter.com/official/en_us/topics/company/2018/Announcing-new-US-issue-ads-policy.html
[232] Jeremy B. Merrill, "How Big Oil Dodges Facebook's New Ad Transparency Rules," *ProPublica*, Nov. 1, 2018, propublica.org/article/how-big-oil-dodges-facebooks-new-ad-transparency-rules
[233] William Turton, "We posed as 100 Senators to run ads on Facebook. Facebook approved all of them.," *Vice News*, Oct. 30, 2018, news.vice.com/en_us/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them?; William Turton, "Facebook's political ad tool let us buy ads 'paid for' by Mike Pence and ISIS," *Vice News*, Oct. 25, 2018, news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis
[234] William Turton, "Facebook's political ad tool let us buy ads 'paid for' by Mike Pence and ISIS," *Vice News*, Oct. 25, 2018, news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis
[235] William Turton, "Facebook's political ad tool let us buy ads 'paid for' by Mike Pence and ISIS," *Vice News*, Oct. 25, 2018, news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis
[236] William Turton, "Facebook's political ad tool let us buy ads 'paid for' by Mike Pence and ISIS," *Vice News*, Oct. 25, 2018, news.vice.com/en_us/article/wj9mny/facebooks-political-ad-tool-let-us-buy-ads-paid-for-by-mike-pence-and-isis
[237] William Turton, "We posed as 100 Senators to run ads on Facebook. Facebook approved all of them.," *Vice News*, Oct. 30, 2018, news.vice.com/en_us/article/xw9n3q/we-posed-as-100-senators-to-run-ads-on-facebook-facebook-approved-all-of-them?
[238] Shona Ghosh, "Cambridge Analytica -- and Facebook failed to catch that they were frauds," *Business Insider*, Oct. 31, 2018, businessinsider.com/facebook-approved-political-ads-paid-for-by-cambridge-analytica-2018-10
[239] "How ads related to politics or issues of national importance are reviewed (with examples)," Facebook Business, accessed Feb. 25, 2019, facebook.com/business/help/313752069181919?helpref=page_content
[240] "Posing as Russian Troll Farm, Watchdog Buys Politically Divisive Ads on Google," Campaign for Accountability, Sept. 4, 2018, campaignforaccountability.org/posing-as-russian-troll-farm-watchdog-buys-politically-divisive-ads-on-google/

[241] Charlie Warzel, "This Group Posed As Russian Trolls And Bought Political Ads on Google. It was Easy.," *Buzzfeed News*, Sept. 4, 2018, buzzfeednews.com/article/charliewarzel/researchers-posed-as-trolls-bought-google-ads
[242] Charlie Warzel, "This Group Posed As Russian Trolls And Bought Political Ads on Google. It was Easy.," *Buzzfeed News*, Sept. 4, 2018, buzzfeednews.com/article/charliewarzel/researchers-posed-as-trolls-bought-google-ads
[243] Amy Sherman, "House Democrats and HR 1: Voting rights expansion or federal power grab?," PolitiFact, Feb. 8, 2019, politifact.com/truth-o-meter/article/2019/feb/08/democrats-seek-expand-voting-access-2020-election-/
[244] Honest Ads Act, S. 1989, 115th Congress (2017-2018)
[245] Heather Timmons and Hanna Kozlowska, "Facebook's quiet battle to kill the first transparency law for online political ads," *Quartz*, March 22, 2018, qz.com/1235363/mark-zuckerberg-and-facebooks-battle-to-kill-the-honest-ads-act/
[246] Honest Ads Act, S. 1989, 115th Congress (2017-2018)
[247] For the People Act of 2019, H. R. 1, 116th Congress (2019-2020)
[248] For the People Act of 2019, H. R. 1, 116th Congress (2019-2020)
[249] For the People Act of 2019, H. R. 1, 116th Congress (2019-2020)
250 Catie Edmondson, "House Passes Democrats' Centerpiece Anti-Corruption and Voting Rights Bill," The New York Times, March 8, 2019,.nytimes.com/2019/03/08/us/politics/house-democrats-anticorruption-voting-rights.html
251 Id.
[252] Tony Romm, "Facebook's new rules aim to thwart the kind of ads bought by Russian trolls during the election," *The Washington Post*, April 6, 2018, washingtonpost.com/news/technology/wp/2018/04/06/facebooks-new-rules-aim-to-thwart-the-kind-of-ads-bought-by-russian-trolls-during-the-election/?utm_term=.3ac49572edaa; see: "Ad Archive," Facebook, accessed Jan. 31, 2019, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=f525457687&e=5cb5c6a55f
[253] Bruce Falck, "Providing more transparency around advertising on Twitter," Twitter Blog, June 28, 2018, blog.twitter.com/official/en_us/topics/company/2018/Providing-More-Transparency-Around-Advertising-on-Twitter.html; see: "Ads Transparency Center," Twitter, accessed Feb. 25, 2019, ads.twitter.com/transparency
[254] Taylor Hatmaker, "Google releases a searchable database of US political ads," *TechCrunch*, Aug. 2018, techcrunch.com/2018/08/15/google-political-ad-library/; see: "Transparency Center," Google, accessed Feb. 25, 2019, transparencyreport.google.com/political-ads/library
[255] Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?," *The New York Times*, Sept. 2, 2018, nytimes.com/2018/09/02/technology/03adarchive.html; "Ad Archive Report," Facebook, accessed Feb. 25, 2019, facebook.com/ads/archive/report/?source=archive-landing-page&country=US; Tony Romm, "Facebook's new rules aim to thwart the kind of ads bought by Russian trolls during the election," *The Washington Post*, April 6, 2018, washingtonpost.com/news/technology/wp/2018/04/06/facebooks-new-rules-aim-to-thwart-the-kind-of-ads-bought-by-russian-trolls-during-the-election/?utm_term=.3ac49572edaa; Bruce Falck, "Providing more transparency around advertising on Twitter," Twitter Blog, June 28, 2018, blog.twitter.com/official/en_us/topics/company/2018/Providing-More-Transparency-Around-Advertising-on-Twitter.html; Taylor Hatmaker, "Google releases a searchable database of US political ads," *TechCrunch*, Aug. 2018, techcrunch.com/2018/08/15/google-political-ad-library/
[256] Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?," *The New York Times*, Sept. 2, 2018, nytimes.com/2018/09/02/technology/03adarchive.html
[257] Jeremy B. Merrill, Ariana Tobin and Madeleine Varner, "What Facebook's New Political Ad System Misses," *ProPublica*, May 24, 2018, propublica.org/article/what-facebooks-new-political-ad-system-misses
[258] Natasha Singer, "Tech Giants Now Share Details on Political Ads. What Does That Mean For You?," *The New York Times*, Sept. 2, 2018, nytimes.com/2018/09/02/technology/03adarchive.html
[259] Jeremy B. Merrill and Ariana Tobin, "Facebook Moves to Block Ad Transparency Tools -- Including Ours," *ProPublica*, Jan. 28, 2019, propublica.org/article/facebook-blocks-ad-transparency-tools%20
[260] See: Jeremy B. Merrill et al., "Facebook Political Ad Collector," *ProPublica*, July 17, 2018, projects.propublica.org/facebook-ads/
[261] Jim Waterson, "Facebook restricts campaigners' ability to check ads for political transparency," *The Guardian*, Jan 27, 2019, theguardian.com/technology/2019/jan/27/facebook-restricts-campaigners-ability-to-check-ads-for-political-transparency
[262] Jeremy B. Merrill and Ariana Tobin, "Facebook Moves to Block Ad Transparency Tools -- Including Ours," *ProPublica*, Jan. 28, 2019, propublica.org/article/facebook-blocks-ad-transparency-tools%20
[263] Jeremy B. Merrill and Ariana Tobin, "Facebook Moves to Block Ad Transparency Tools -- Including Ours," *ProPublica*, Jan. 28, 2019, propublica.org/article/facebook-blocks-ad-transparency-tools%20

[264] "Klobuchar Statement on Facebook's Actions to Implement Honest Ads Act," News Releases, United States Senator Amy Klobuchar, April 6, 2018, klobuchar.senate.gov/public/index.cfm/2018/4/klobuchar-statement-on-facebook-s-actions-to-implement-honest-ads-act
[265] "Issues of national importance," Facebook Business, accessed Feb. 25, 2019, facebook.com/business/help/214754279118974?helpref=faq_content
[266] David Beard, "How Facebook tried to block distribution of a blockbuster story," *Poynter*, June 25, 2018, poynter.org/newsletters/2018/how-facebook-tried-to-block-distribution-of-a-blockbuster-story/
[267] David Beard, "How Facebook tried to block distribution of a blockbuster story," *Poynter*, June 25, 2018, poynter.org/newsletters/2018/how-facebook-tried-to-block-distribution-of-a-blockbuster-story/
[268] Jeremy B. Merrill and Ariana Tobin, "Facebook's Screening for Political Ads Nabs News Sites Instead of Politicians," *ProPublica*, June 15, 2018, propublica.org/article/facebook-new-screening-system-flags-the-wrong-ads-as-political
[269] See: Jean Guerrero, "Child Faces Immigration Judge Without her Parents In San Diego," *KPBS*, July 10, 2018, kpbs.org/news/2018/jul/10/child-faces-immigration-judge-without-her-parents-/?utm_content=buffer9857f&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer
[270] Jean Guerrero (@jeanguerre), "Facebook is censoring my nonprofit news org, @KPBSnews," Twitter, July 12, 2018, twitter.com/jeanguerre/status/1017509787037155328
[271] See: Mike Snider and Jessica Guynn, "News publishers protest Facebook's new political ad rules," *USA Today*, May 18, 2018, usatoday.com/story/tech/news/2018/05/18/news-publishers-protest-facebooks-new-political-ad-rules/623241002/
[272] Lucia Moses, "Publishers stop Facebook ad spending over policy that treats publishers as political advertisers," *Digiday*, May 25, 2018, digiday.com/media/financial-times-stops-facebook-ad-spending-policy-treats-publishers-political-advertisers/
[273] Lucia Moses, "Seven news organizations protest Facebook's issue ads policy," *Digiday*, June 11, 2018, digiday.com/media/seven-news-organizations-protest-facebooks-issue-ads-policy/
[274] American Society to New Editors *et al*, Open Letter to Mark Zuckerberg, June 11, 2018, newsmediaalliance.org/wp-content/uploads/2018/06/Alternative-Facebook-Politics-Tagging-Solutions-FINAL.pdf
[275] Lucia Moses, "Seven news organizations protest Facebook's issue ads policy," *Digiday*, June 11, 2018, digiday.com/media/seven-news-organizations-protest-facebooks-issue-ads-policy/
[276] Lucia Moses, "Facebook tweaks political ads policy, but not enough to satisfy irate publishers," *Digiday*, June 28, 2018, digiday.com/media/facebook-tweaks-political-ads-policy-not-enough-satisfy-irate-publishers/
[277] "Authorizing Ads with Political Content: Why Publishers Are Included," Facebook for Media, June 13, 2018, facebook.com/facebookmedia/blog/authorizing-ads-with-political-content-why-publishers-are-included
[278] Lucia Moses, "Facebook tweaks political ads policy, but not enough to satisfy irate publishers," *Digiday*, June 28, 2018, digiday.com/media/facebook-tweaks-political-ads-policy-not-enough-satisfy-irate-publishers/
[279] "Ad Archive," Facebook, accessed Jan. 31, 2019, list-manage.us13.list-manage.com/track/click?u=986b63cc0ee0561c292118500&id=f525457687&e=5cb5c6a55f
[280] Lucia Moses and Kerry Flynn, "Twitter tweaks Facebook with new issue ads policy that exempts publishers," *Digiday*, Aug. 30, 2018, digiday.com/media/twitter-creates-issue-ads-policy-that-exempts-publishers-from-issue-ads-policy-in-contrast-with-facebook/
[281] Nathaniel Gleicher, "How We Work With Our Partners to Combat Information Operations," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[282] Sarah Frier, Selina Wang, Alyza Sebenius, "Facebook's Secret Weapon for Fighting Election Interference: The Government," Bloomberg, November 11, 2018, bloomberg.com/news/articles/2018-11-11/facebook-s-secret-weapon-for-fighting-election-interference-the-government
[283] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[284] Donie O'Sullivan, "Twitter took down thousands of accounts that discouraged voting in midterms," *CNN*, Nov. 3, 2018, cnn.com/2018/11/02/tech/twitter-accounts-discourage-voting/index.html
[285] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[286] Sarah Frier, Selina Wang and Alyza Sebenius, "Facebook's Secret Weapon for Fighting Election Interference: The Government," *Bloomberg*, Nov. 11, 2018, bloomberg.com/news/articles/2018-11-11/facebook-s-secret-weapon-for-fighting-election-interference-the-government
[287] Handling requests from governments around the world that act with a range of motives and with widely varying respect for human rights is obviously a major challenge for Facebook and other social media platforms. PEN America tracks these issues as well, but within the context of this report about U.S. elections, we are limiting our commentary to the social media platforms' collaboration with U.S. government agencies.

[288] Nathaniel Gleicher, "How We Work With Our Partners to Combat Information Operations," Facebook Newsroom, Nov. 13, 2018, newsroom.fb.com/news/2018/11/last-weeks-takedowns/
[289] Google spokesperson, interviewed by PEN America, February 13, 2019 (email).
[290] Id. Google's transparency report is available at https://transparencyreport.google.com/
[291] Facebook spokesperson, interviewed by PEN America, February 11, 2019 (by phone and email).
[292] Id. The Transparency Report is publicly available at https://transparency.facebook.com/.
[293] Twitter Spokesperson, interviewed by PEN America, February 25, 2019 (email). Twitter's Transparency Report is available at https://transparency.twitter.com/en.html, and its legal request FAQ is available at https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs
[294] Daniel Kreiss and Shannon C. McGregor, "Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle," *Political Communication* 35, no. 2 (Oct. 26, 2017): 155-177, doi.org/10.1080/10584609.2017.1364814
[295] Nancy Scola, "How Facebook, Google and Twitter 'embeds' helped Trump in 2016," *Politico*, Oct. 26, 2017, politico.com/story/2017/10/26/facebook-google-twitter-trump-244191
[296] Lois Beckett, "Trump digital director says Facebook helped win the White House," *The Guardian*, Oct. 8, 2017, theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising
[297] Elliot Schrage, "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/
[298] Facebook spokesperson, interviewed by PEN America, February 11, 2019 (by phone and email)
[299] Twitter Spokesperson, interviewed by PEN America, February 25, 2019 (email)
[300] See e.g. Scott Horsley and Miles Parks, "Trump's Refusal To Back U.S. Intel Over Russia At Putin Summit Sparks Bipartisan Ire," *NPR*, July 16, 2018, npr.org/2018/07/16/628973563/trump-putin-to-meet-after-new-charges-over-russias-2016-election-interference; Deb Riechmann, "Trump criticized for not leading effort to secure elections," *Associated Press*, Aug. 1, 2018, apnews.com/89521f7d441b441597ef6e6d79c58be7; Ashley Wood, "The Politics of Trump's Mismatched Response to Election Interference," Just Security, Oct. 2, 2018, justsecurity.org/60926/politics-trumps-mismatched-response-election-interference/
[301] Deb Riechmann, "Trump criticized for not leading effort to secure elections," *Associated Press*, Aug. 1, 2018, apnews.com/89521f7d441b441597ef6e6d79c58be7
[302] "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," The White House, Sept. 12, 2018, whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/; see also: Jeff Mason, "Trump signs order to enable sanctions for U.S. election meddling," *Reuters*, Sept. 12, 2018, reuters.com/article/us-usa-cyber-election/trump-signs-order-to-enable-sanctions-for-u-s-election-meddling-idUSKCN1LS2NA
[303] "Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," The White House, Sept. 12, 2018, whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/
[304] "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," Office of the Director of National Intelligence, Oct. 19, 2018, dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections
[305] "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," Office of the Director of National Intelligence, Oct. 19, 2018, dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections
[306]"Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," Office of the Director of National Intelligence, Oct. 19, 2018, dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections
[307] Pete Williams and Ken Dilanian, "DHS finds increasing attempts to hack U.S. election systems ahead of midterms," *NBC News*, Oct. 15, 2018, nbcnews.com/politics/national-security/dhs-finds-increasing-attempts-hack-u-s-election-systems-ahead-n920336
[308] "DNI Coats Statement on the IC's Response to EO 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a U.S. Election," Office of the Director of National Intelligence, Dec. 21, 2018, dni.gov/index.php/newsroom/press-releases/item/1933-dni-coats-statement-on-the-intelligence-community-s-response-to-executive-order-13848-on-imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election
[309] Phil Stewart, "Pentagon chief slams 'slow learner' Putin over election meddling," *Reuters*, Dec. 1, 2018, reuters.com/article/us-usa-russia-mattis/pentagon-chief-slams-slow-learner-putin-over-election-meddling-idUSKCN1O03U8
[310] Ellen Nakashima, "NSA and Cyber Command to coordinate actions to counter Russian election interference in 2018 amid absence of White House guidance," Washington Post, July 17, 2018, washingtonpost.com/world/national-security/nsa-and-cyber-command-to-coordinate-actions-to-counter-russian-

election-interference-in-2018-amid-absence-of-white-house-guidance/2018/07/17/baac95b2-8900-11e8-85ae-511bc1146b0b_story.html?utm_term=.1b7aa1b4f39e

[311] Ellen Nakashima, "NSA and Cyber Command to coordinate actions to counter Russian election interference in 2018 amid absence of White House guidance," Washington Post, July 17, 2018, washingtonpost.com/world/national-security/nsa-and-cyber-command-to-coordinate-actions-to-counter-russian-election-interference-in-2018-amid-absence-of-white-house-guidance/2018/07/17/baac95b2-8900-11e8-85ae-511bc1146b0b_story.html?utm_term=.1b7aa1b4f39e

[312] "Combating Foreign Influence," FBI, accessed Feb. 25, 2019, fbi.gov/investigate/counterintelligence/foreign-influence

[313] "Combating Foreign Influence," FBI, accessed Feb. 25, 2019, fbi.gov/investigate/counterintelligence/foreign-influence

[314] "FBI Director Christopher Wray's Statement at Press Briefing on Election Security," FBI News, Aug. 2, 2018, fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-statement-at-press-briefing-on-election-security

[315] John Frank, "The FBI is training political campaigns to fight foreign influence in Colorado elections. And here's what voters can do.," *The Colorado Sun*, Sept. 11, 2018, coloradosun.com/2018/09/11/fbi-colorado-election-hack/

[316] Mike Weissman, interview by PEN America, October 25, 2018 (by phone)

[317] Mike Weissman, interview by PEN America, October 25, 2018 (by phone)

[318] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *The New York Times*, Oct. 23, 2018, nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?action=click&module=Top%20Stories&pgtype=Homepage

[319] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *The New York Times*, Oct. 23, 2018, nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?action=click&module=Top%20Stories&pgtype=Homepage

[320] Nina Jankowicz, interview by PEN America interview, Oct. 25, 2018 (in person)

[321] Zachary Fryer-Biggs, "The Pentagon Has Prepared a Cyber-Attack Against Russia," *The Daily Beast*, November 2, 2018, thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia?via=newsletter&source=DDMorning.

[322] Zachary Fryer-Biggs, "The Pentagon Has Prepared a Cyber-Attack Against Russia," *The Daily Beast,* November 2, 2018, thedailybeast.com/the-pentagon-has-prepared-a-cyber-attack-against-russia?via=newsletter&source=DDMorning.

[323] Ellen Nakashima, " U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," Washington Post, Feb. 27, 2019, washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.084557036fc9

[324] *Id.*

[325] *Id.*

[326] *Id.*

[327] "U.S. cyber-attacks will accelerate Russia's efforts to create a Chinese-style firewall," The Bell, March 1, 2019, thebell.io/en/u-s-cyber-attacks-will-accelerate-russia-s-efforts-to-create-a-chinese-style-firewall/

[328]"Joint Statement on Election Day Preparations," Homeland Security, Nov. 5, 2018, dhs.gov/cisa/news/2018/11/05/joint-statement-election-day-preparations

[329] "Joint Statement on Election Day Preparations," Homeland Security, Nov. 5, 2018, dhs.gov/news/2018/11/05/joint-statement-election-day-preparations

[330] "Joint Statement on Election Day Preparations," Homeland Security, Nov. 5, 2018, dhs.gov/news/2018/11/05/joint-statement-election-day-preparations

[331] See: Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf

[332] Alex Stamos, "How the U.S. Has Failed to Protect the 2018 Election--and Four Ways to Protect 2020," *Lawfare*, Aug. 22, 2018, lawfareblog.com/how-us-has-failed-protect-2018-election-and-four-ways-protect-2020

[333] Alex Stamos, "How the U.S. Has Failed to Protect the 2018 Election--and Four Ways to Protect 2020," *Lawfare*, Aug. 22, 2018, lawfareblog.com/how-us-has-failed-protect-2018-election-and-four-ways-protect-2020

[334] Alex Stamos, "How the U.S. Has Failed to Protect the 2018 Election--and Four Ways to Protect 2020," *Lawfare*, Aug. 22, 2018, lawfareblog.com/how-us-has-failed-protect-2018-election-and-four-ways-protect-2020

[335] Ashley Deeks, Sabrina McCubbin and Cody M. Poplin, "Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?," *Lawfare*, Oct. 25, 2017, lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts

[336] Ashley Deeks, Sabrina McCubbin and Cody M. Poplin, "Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?," *Lawfare*, Oct. 25, 2017, lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts
[337] *See* Alex Seitz-Wald, "Democratic Party sues Trump, Russia, Wikileaks over 2016 email hack," *NBC News*, April 20, 2018, nbcnews.com/politics/donald-trump/dnc-sues-trump-russia-wikileaks-over-2016-email-hack-n867801
[338] Seema Nanda, "100 Days Out, 10 DNC Efforts You Need to Know About," DNC, July 27, 2018, documentcloud.org/documents/4620716-Memo-100-Days.html
[339] Hadas Gold, "DNC tech chief says no successful hacking attempts were seen in the midterms," *CNN*, Nov. 8, 2018, cnn.com/2018/11/08/politics/dnc-hacking-midterms/index.html
[340] Hadas Gold, "DNC tech chief says no successful hacking attempts were seen in the midterms," *CNN*, Nov. 8, 2018, cnn.com/2018/11/08/politics/dnc-hacking-midterms/index.html
[341] Hadas Gold, "DNC tech chief says no successful hacking attempts were seen in the midterms," *CNN*, Nov. 8, 2018, cnn.com/2018/11/08/politics/dnc-hacking-midterms/index.html
[342] Elizabeth Schulze, "Fake news 'to get worse' by 2020 election unless social media firms act, DNC tech chief says," *CNBC*, Nov. 8, 2018, cnbc.com/2018/11/08/fake-news-is-going-to-get-worse-unless-companies-take-action-dnc-cto.html
[343] sp.a, "Teken de Klimaatpetitie," Facebook, May 20, 2018, facebook.com/watch/?v=10155618434657151
[344] Oscar Schwartz, "You thought fake news was bad? Deep fakes are where truth goes to die," *The Guardian*, Nov. 12, 2018, theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[345] Oscar Schwartz, "You thought fake news was bad? Deep fakes are where truth goes to die," *The Guardian*, Nov. 12, 2018, theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[346] Oscar Schwartz, "You thought fake news was bad? Deep fakes are where truth goes to die," *The Guardian*, Nov. 12, 2018, theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[347] Oscar Schwartz, "You thought fake news was bad? Deep fakes are where truth goes to die," *The Guardian*, Nov. 12, 2018, theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[348] Renee DiResta, et al., "The Tactics & Tropes of the Internet Research Agency," New Knowledge, disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf
[349] "Junk news dominating coverage of US midterms on social media, new research finds," Oxford Internet Institute, Nov. 1, 2018, oii.ox.ac.uk/news/releases/junk-news-dominating-coverage-of-us-midterms-on-social-media-new-research-finds/
[350] Nahema Marchal et al., "Polarization, Partisanship and Junk News Consumption on Social Media During the 2018 US Midterm Elections," Oxford University, Nov. 1, 2018, blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2018/11/marchal_et_al.pdf
[351] "Junk news dominating coverage of US midterms on social media, new research finds," Oxford Internet Institute, Nov. 1, 2018, oii.ox.ac.uk/news/releases/junk-news-dominating-coverage-of-us-midterms-on-social-media-new-research-finds/
[352] Nahema Marchal et al., "Polarization, Partisanship and Junk News Consumption on Social Media During the 2018 US Midterm Elections," Oxford University, Nov. 1, 2018, blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2018/11/marchal_et_al.pdf. See p. 2 for the study's typology of content classification.
[353] "Junk news dominating coverage of US midterms on social media, new research finds," Oxford Internet Institute, Nov. 1, 2018, oii.ox.ac.uk/news/releases/junk-news-dominating-coverage-of-us-midterms-on-social-media-new-research-finds/
[354] Craig Timberg and Tony Romm, "Forget the Russians. On this Election Day, it's Americans peddling disinformation and hate speech.," *The Washington Post*, Nov. 6, 2018, washingtonpost.com/technology/2018/11/06/forget-russians-this-election-day-its-americans-peddling-disinformation-hate-speech/?utm_term=.eca80741c69d
[355] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[356] Sheera Frenkel, "Facebook Tackles Rising Threat: Americans Aping Russian Schemes to Deceive," *The New York Times*, Oct. 11, 2018, nytimes.com/2018/10/11/technology/fake-news-online-disinformation.html
[357] PEN America interview with Graham Brookie, Oct. 25, 2018 (phone)
[358] Dustin Volz, "No Significant Foreign Interference Seen on Midterm Vote," *The Wall Street Journal*, Nov. 7, 2018, wsj.com/articles/u-s-on-alert-for-election-interference-says-nothing-significant-spotted-1541521048?emailToken=38dd5cc1303345e4b8dcf9f2be2399d5yjrcHaTJtEMP5HCCncixvFJ44MV/Wu4uY6TB/D9RelFrk2IRLzERAZnjcncdWI7AUYGTitex1cgTr3kuoPyAOnu2TjIf&ns=prod/accounts-wsj
[359] Dustin Volz, "No Significant Foreign Interference Seen on Midterm Vote," *The Wall Street Journal*, Nov. 7, 2018, wsj.com/articles/u-s-on-alert-for-election-interference-says-nothing-significant-spotted-

1541521048?emailToken=38dd5cc1303345e4b8dcf9f2be2399d5yjrcHaTJtEMP5HCCncixvFJ44MV/Wu4uY6TB/D9RelFrk2IRLzERAZnjcncdWI7AUYGTitex1cgTr3kuoPyAOnu2TjIf&ns=prod/accounts-wsj

[360] Dustin Volz, "No Significant Foreign Interference Seen on Midterm Vote," *The Wall Street Journal*, Nov. 7, 2018, wsj.com/articles/u-s-on-alert-for-election-interference-says-nothing-significant-spotted-1541521048?emailToken=38dd5cc1303345e4b8dcf9f2be2399d5yjrcHaTJtEMP5HCCncixvFJ44MV/Wu4uY6TB/D9RelFrk2IRLzERAZnjcncdWI7AUYGTitex1cgTr3kuoPyAOnu2TjIf&ns=prod/accounts-wsj

[361] Renée DiResta, "What We Now Know About Russian Disinformation," *The New York Times*, Dec. 17, 2018, nytimes.com/2018/12/17/opinion/russia-report-disinformation.html

[362] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download?

[363] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 4)

[364] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (e.g. pg. 14, "Between in or around December 2016 and in or around May 2018, as part of the Conspiracy's effort to sow discord in the U.S. political system, members of the Conspiracy used social media and other internet platforms to inflame passions on a wide variety of topics,")

[365] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download?

[366] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 13)

[367] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 14)

[368] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 37)

[369] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 37)

[370] *United States of America v. Elena Alekseevna Khusyaynova*, 1:18-MJ-464 (Virginia 2018) justice.gov/opa/press-release/file/1102316/download? (page 34)

[371] PEN America interview with Renee DiResta on Oct. 18, 2018 (phone)

[372] Kevin Roose, "Is a New Russian Meddling Tactic Hiding in Plain Sight?," *The New York Times*, Sept. 25, 2018, nytimes.com/2018/09/25/technology/usareally-russian-news-site-propaganda.html?

[373] "About Us," USA Really, accessed Feb. 26, 2019, usareally.com/page/contacts

[374] Kevin Roose, "Is a New Russian Meddling Tactic Hiding in Plain Sight?," *The New York Times*, Sept. 25, 2018, nytimes.com/2018/09/25/technology/usareally-russian-news-site-propaganda.html?

[375] Kevin Roose, "Is a New Russian Meddling Tactic Hiding in Plain Sight?," *The New York Times*, Sept. 25, 2018, nytimes.com/2018/09/25/technology/usareally-russian-news-site-propaganda.html?; see also: Sergey Petrov, "'Wake Up America' - FAN is Preparing to Launch a New News Agency," Federal News Agency, April 4, 2018, riafan.ru/1043445-prosnis-amerika-fan-gotovit-k-zapusku-novoe-informacionnoe-agentstvo

[376] Kevin Roose, "Is a New Russian Meddling Tactic Hiding in Plain Sight?," *The New York Times*, Sept. 25, 2018, nytimes.com/2018/09/25/technology/usareally-russian-news-site-propaganda.html?

[377] See: RT, Facebook, accessed Feb. 26, 2018, facebook.com/RTnews/

[378] Angelo Fichera, "Doctored Image Takes Aim at Stacey Abrams," FactCheck.org, Oct. 8, 2018, factcheck.org/2018/10/doctored-image-takes-aim-at-stacey-abrams/

[379] Angelo Fichera, "Doctored Image Takes Aim at Stacey Abrams," FactCheck.org, Oct. 8, 2018, factcheck.org/2018/10/doctored-image-takes-aim-at-stacey-abrams/

[380] Angelo Fichera, "Doctored Image Takes Aim at Stacey Abrams," FactCheck.org, Oct. 8, 2018, factcheck.org/2018/10/doctored-image-takes-aim-at-stacey-abrams/

[381] Angelo Fichera, "Doctored Image Takes Aim at Stacey Abrams," FactCheck.org, Oct. 8, 2018, factcheck.org/2018/10/doctored-image-takes-aim-at-stacey-abrams/

[382] Angelo Fichera, "Doctored Image Takes Aim at Stacey Abrams," FactCheck.org, Oct. 8, 2018, factcheck.org/2018/10/doctored-image-takes-aim-at-stacey-abrams/

[383] Kyra Haas, "Ted Cruz didn't blame gay people for mass shootings and public nudity," PolitiFact, Sept. 17, 2018, politifact.com/facebook-fact-checks/statements/2018/sep/17/viral-image/ted-cruz-didnt-blame-gay-people-mass-shootings-and/

[384] A post of this meme is available at pbs.twimg.com/media/DZ5mwuFX4AIgJG1.jpg:large
[385] Kyra Haas, "Ted Cruz didn't blame gay people for mass shootings and public nudity," PolitiFact, Sept. 17, 2018, politifact.com/facebook-fact-checks/statements/2018/sep/17/viral-image/ted-cruz-didnt-blame-gay-people-mass-shootings-and/
[386] Kyra Haas, "Ted Cruz didn't blame gay people for mass shootings and public nudity," PolitiFact, Sept. 17, 2018, politifact.com/facebook-fact-checks/statements/2018/sep/17/viral-image/ted-cruz-didnt-blame-gay-people-mass-shootings-and/
[387] Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About The Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[388] Miriam Valverde, "Facebook meme falsely attributes quote about race, slaves and Islam to Ilhan Omar," PolitiFact, Nov. 15, 2018, politifact.com/facebook-fact-checks/statements/2018/nov/15/viral-image/facebook-meme-falsely-attributes-quote-ilhan-omar/
[389] Miriam Valverde, "Facebook meme falsely attributes quote about race, slaves and Islam to Ilhan Omar," PolitiFact, Nov. 15, 2018, politifact.com/facebook-fact-checks/statements/2018/nov/15/viral-image/facebook-meme-falsely-attributes-quote-ilhan-omar/ ; see also: "How is Facebook addressing false news through third-party fact checkers?," Facebook Help Center, accessed Feb. 26, 2019, facebook.com/help/1952307158131536?
[390] facebook.com/photo.php?fbid=10215617473164691&set=a.2866015564293&type=3&theater (leading to a "content not available" page)
[391] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html; abcnews.go.com/US/roy-moores-accusers-responses/story?id=51138718
[392] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[393] Joe Tacopino, "Roy Moore flooded with fake Russian Twitter followers," *New York Post*, Oct. 16, 2017, nypost.com/2017/10/16/roy-moore-flooded-with-fake-russian-twitter-followers/; David Weigel, "Roy Moore's Senate campaign blames Democrats for fake Twitter followers," *The Washington Post*, Oct. 16, 2017, washingtonpost.com/news/powerpost/wp/2017/10/16/roy-moores-senate-campaign-gets-twitter-to-delete-thousands-of-fake-followers/?utm_term=.e235c167e915
[394] Joe Tacopino, "Roy Moore flooded with fake Russian Twitter followers," *New York Post*, Oct. 16, 2017, nypost.com/2017/10/16/roy-moore-flooded-with-fake-russian-twitter-followers/
[395] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[396] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html; Tony Romm and Craig Timberg, "Facebook suspends five accounts, including that of a social media researcher, for misleading tactics in Alabama election," *The Washington Post*, Dec. 22, 2018, washingtonpost.com/technology/2018/12/22/facebook-suspends-five-accounts-including-social-media-researcher-misleading-tactics-alabama-election/?
[397] Jonathon Morgan, "Social Media and the Alabama Special Election," *Medium*, Jan. 2, 2019, medium.com/@jonathonmorgan/social-media-and-the-alabama-special-election-c83350324529
[398] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[399] Tony Romm, Craig Timberg and Aaron C. Davis, "Internet billionaire Reid Hoffman apologizes for funding a group tied to disinformation in Alabama race," *The Washington Post*, Dec. 26, 2018, washingtonpost.com/technology/2018/12/26/internet-billionaire-reid-hoffman-apologizes-funding-group-behind-disinformation-alabama-race/?utm_term=.54479124753f; Reid Hoffman, "Truth and Politics," *Medium*, Dec. 26, 2018, medium.com/@reidhoffman/truth-and-politics-1a532bc6c2b1
[400] Jonathon Morgan, "Social Media and the Alabama Special Election," *Medium*, Jan. 2, 2019, medium.com/@jonathonmorgan/social-media-and-the-alabama-special-election-c83350324529
[401] Scott Shane, "Facebook Closes 5 Accounts Tied to Russia-Like Tactics in Alabama Senate Race," *The New York Times*, Dec. 22, 2018, nytimes.com/2018/12/22/us/politics/facebook-suspends-alabama-elections.html
[402] Scott Shane, "Facebook Closes 5 Accounts Tied to Russia-Like Tactics in Alabama Senate Race," *The New York Times*, Dec. 22, 2018, nytimes.com/2018/12/22/us/politics/facebook-suspends-alabama-elections.html
[403] Craig Timberg, Tony Romm and Aaron C. Davis, "Researcher whose firm wrote report on Russian interference used questionable online tactics during Ala. Senate race," *The Washington Post*, Dec. 18, 2018, washingtonpost.com/technology/2018/12/19/researcher-affiliated-with-russian-interference-senate-report-used-questionable-online-tactics-during-alabama-senate-race/?utm_term=.b43e55ad6871; Ellen Ioanes, "Social media researcher says he tried Russian-style influence tactics in Alabama," *The Daily Dot*, Dec. 19, 2018, dailydot.com/layer8/alabama-facebook-new-knowledge-jonathon-morgan/

[404] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[405] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[406] Scott Shane and Alan Blinder, "Secret Experiment in Alabama Senate Race Imitated Russian Tactics," *The New York Times*, Dec. 19, 2018, nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html
[407] Scott Shane and Alan Blinder, "Democrats Faked Online Push to Outlaw Alcohol in Alabama Race," *The New York Times*, Jan. 7, 2019, nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html
[408] Scott Shane and Alan Blinder, "Democrats Faked Online Push to Outlaw Alcohol in Alabama Race," *The New York Times*, Jan. 7, 2019, nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html
[409] "Democrats used Russian tactics in Alabama. Now they must swear them off.," *The Washington Post*, Dec. 27, 2018, washingtonpost.com/opinions/democrats-used-russian-tactics-in-alabama-now-they-must-swear-them-off/2018/12/27/5b97c332-0941-11e9-a3f0-71c95106d96a_story.html?utm_term=.3cb348146b5d
[410] "Democrats used Russian tactics in Alabama. Now they must swear them off.," *The Washington Post*, Dec. 27, 2018, washingtonpost.com/opinions/democrats-used-russian-tactics-in-alabama-now-they-must-swear-them-off/2018/12/27/5b97c332-0941-11e9-a3f0-71c95106d96a_story.html?utm_term=.3cb348146b5d
[411] Scott Shane and Alan Blinder, "Democrats Faked Online Push to Outlaw Alcohol in Alabama Race," *The New York Times*, Jan. 7, 2019, nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html
[412] Kevin Roose, "We Asked for Examples of Election Disinformation. You Delivered.," *The New York Times*, Nov. 4, 2018, nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html
[413] Millionaire Claire (@Millions4Claire), Twitter, accessed Feb. 26, 2019, twitter.com/millions4claire
[414] Kevin Roose, "We Asked for Examples of Election Disinformation. You Delivered.," *The New York Times*, Nov. 4, 2018, nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html
[415] Id.
[416] Kevin Roose, "We Asked for Examples of Election Disinformation. You Delivered.," *The New York Times*, Nov. 4, 2018, nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html
[417] See: Kevin Roose, "We Asked for Examples of Election Disinformation. You Delivered.," *The New York Times*, Nov. 4, 2018, nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html
[418] Kevin Roose, "Debunking 5 Viral Rumors About Christine Blasey Ford, Kavanaugh's Accuser," *The New York Times*, Sept. 19, 2018, nytimes.com/2018/09/19/us/politics/christine-blasey-ford-kavanaughs-fact-check.html?; Kevin Roose, "Debunking 5 (More) Viral Rumors About Kavanaugh's Accusers," *The New York Times*, Sept. 26, 2018, nytimes.com/2018/09/26/us/politics/kavanaugh-fact-check.html?
[419] Kevin Roose, "Debunking 5 (More) Viral Rumors About Kavanaugh's Accusers," *The New York Times*, Sept. 26, 2018, nytimes.com/2018/09/26/us/politics/kavanaugh-fact-check.html?
[420] Patrick Howley, "BUSTED: Kavanaugh Second Accuser Was George Soros Open Society Fellow," archive.today, Sept. 24, 2018, archive.fo/l4yMZ
[421] Kevin Roose, "Debunking 5 (More) Viral Rumors About Kavanaugh's Accusers," *The New York Times*, Sept. 26, 2018, nytimes.com/2018/09/26/us/politics/kavanaugh-fact-check.html?
[422] Kevin Roose, "Debunking 5 (More) Viral Rumors About Kavanaugh's Accusers," *The New York Times*, Sept. 26, 2018, nytimes.com/2018/09/26/us/politics/kavanaugh-fact-check.html?
[423] Kevin Roose, "Debunking 5 Viral Rumors About Christine Blasey Ford, Kavanaugh's Accuser," *The New York Times*, Sept. 19, 2018, nytimes.com/2018/09/19/us/politics/christine-blasey-ford-kavanaughs-fact-check.html?
[424] Ben Collins, "Far-right news sites smear California professor after misidentifying Kavanaugh accuser," *NBC News*, Sept. 17, 2018, nbcnews.com/tech/tech-news/far-right-news-sites-smear-california-professor-after-misidentifying-kavanaugh-n910471
[425] Kevin Roose, "Debunking 5 Viral Rumors About Christine Blasey Ford, Kavanaugh's Accuser," *The New York Times*, Sept. 19, 2018, nytimes.com/2018/09/19/us/politics/christine-blasey-ford-kavanaughs-fact-check.html?; "'Something's Wrong With Her': Christine Ford's Students Savage Her in Reviews [Story Retracted]," *Grabien*, Sept. 17, 2018, news.grabien.com/story-somethings-wrong-her-christine-fords-students-savage-her-rev
[426] See: Steven Portnoy (@stevenportnoy), "@CBSNews went to Montgomery Co Court today to look into Blasey's parents' 1996 foreclosure," Twitter, Sept. 17, 2018, twitter.com/stevenportnoy/status/1041783867290644480; "Did Judge Martha Kavanaugh 'Rule Against' the Parents of Her Son's Accuser, Christine Blasey-Ford?," Snopes, accessed Feb. 26, 2019, snopes.com/fact-check/brett-kavanaugh-foreclosure-accuser-parents/
[427] Jim Hoft, "Bad Blood: Judge Kavanaugh's Mother Presided Over Far Left Accuser's Parents' Home Foreclosure," *Gateway Pundit*, Sept. 17, 2018, thegatewaypundit.com/2018/09/bad-blood-judge-kavanaughs-mother-foreclosed-on-far-left-accusers-parents-home/
[428] Chris Cillizza, "What Trump has stopped talking about since Election Day," *CNN*, Nov. 14, 2018, cnn.com/2018/11/14/politics/donald-trump-caravan/index.html

[429] Chris Cillizza, "What Trump has stopped talking about since Election Day," *CNN*, Nov. 14, 2018, cnn.com/2018/11/14/politics/donald-trump-caravan/index.html
[430] Donald J. Trump (@realDonaldTrump), "Sadly, it looks like Mexico's Police and Military are unable to stop the Caravan heading to the Southern Border of the United States," Twitter, Oct. 22, 2018, twitter.com/realDonaldTrump/status/1054351078328885248?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1054351078328885248&ref_url=https%3A%2F%2Fwww.cnbc.com%2F2018%2F10%2F22%2Ftrump-says-unknown-middle-easterners-are-mixed-in-migrant-caravan.html; see: Tasneem Nashrulla, "Trump Tweeted An Unverified Claim About 'Unknown Middle Easterners' In the Caravan -- An Idea That Began As Terrorist Fearmongering," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/tasneemnashrulla/trump-claim-caravan-unknown-middle-easterners
[431] Tasneem Nashrulla, "Trump Tweeted An Unverified Claim About 'Unknown Middle Easterners' In the Caravan -- An Idea That Began As Terrorist Fearmongering," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/tasneemnashrulla/trump-claim-caravan-unknown-middle-easterners
[432] Tasneem Nashrulla, "Trump Tweeted An Unverified Claim About 'Unknown Middle Easterners' In the Caravan -- An Idea That Began As Terrorist Fearmongering," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/tasneemnashrulla/trump-claim-caravan-unknown-middle-easterners
[433] Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About the Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[434] Kevin Roose, "We Asked for Examples of Election Disinformation. You Delivered.," *The New York Times*, Nov. 4, 2018, nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html
[435] Jane Lytvynenko and Hayes Brown, "We're Tracking Misinformation About the Migrant Caravan Headed To The US," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/janelytvynenko/were-tracking-misinformation-about-the-migrant-caravan
[436] Donald J. Trump (@realDonaldTrump), "Can you believe this, and what Democrats are allowing to be done to our Country?," Twitter, Oct. 18, 2018, twitter.com/realDonaldTrump/status/1053013864244219904
[437] Jane Lytvynenko and Hayes Brown, "We're Tracking Misinformation About the Migrant Caravan Headed To The US," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/janelytvynenko/were-tracking-misinformation-about-the-migrant-caravan
[438] Jane Lytvynenko and Hayes Brown, "We're Tracking Misinformation About the Migrant Caravan Headed To The US," *Buzzfeed News*, Oct. 22, 2018, buzzfeednews.com/article/janelytvynenko/were-tracking-misinformation-about-the-migrant-caravan
[439] Ken Bensinger and Karla Zabludovsky, "A Mysterious Imposter Account Was Used On Facebook To Drum Up Support For The Migrant Caravan," *Buzzfeed News*, Dec. 6, 2018, buzzfeednews.com/article/kenbensinger/a-mysterious-imposter-account-was-used-on-facebook-to-drum
[440] Ken Bensinger and Karla Zabludovsky, "A Mysterious Imposter Account Was Used On Facebook To Drum Up Support For The Migrant Caravan," *Buzzfeed News*, Dec. 6, 2018, buzzfeednews.com/article/kenbensinger/a-mysterious-imposter-account-was-used-on-facebook-to-drum
[441] Young Mie Kim, "Voter Suppression Has Gone Digital," Brennan Center for Justice, Nov. 20, 2018, brennancenter.org/blog/voter-suppression-has-gone-digital
[442] "Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States," January 31, 2019, blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf
[443] Brian Ries et al., "Election Night in the US," *CNN*, Nov. 7, 2018, edition.cnn.com/politics/live-news/election-day-2018/h_e600998ef988388f92994330ee20861;
[444] ICE (@ICEgov), "ICE does not patrol or conduct enforcement operations at polling locations," Twitter, Nov. 6, 2018, twitter.com/ICEgov/status/1059888145955729408
[445] Young Mie Kim, "Voter Suppression Has Gone Digital," Brennan Center for Justice, Nov. 20, 2018, brennancenter.org/blog/voter-suppression-has-gone-digital
[446] Id. *See also* "Judge strikes down Kansas law requiring proof of citizenship to vote," Associated Press, June 18, 2018, nbcnews.com/news/crime-courts/judge-strikes-down-kansas-law-requiring-proof-citizenship-vote-n884516
[447] Jane Lytvynenko, "North Dakota Democrats Ran A Misleading Facebook Ad Discouraging People From Voting," *Buzzfeed News*, Nov. 2, 2018, buzzfeednews.com/article/janelytvynenko/north-dakota-democrats-facebook-ad-voter-suppression
[448] Jane Lytvynenko, "North Dakota Democrats Ran A Misleading Facebook Ad Discouraging People From Voting," *Buzzfeed News*, Nov. 2, 2018, buzzfeednews.com/article/janelytvynenko/north-dakota-democrats-facebook-ad-voter-suppression
[449] Jane Lytvynenko, "North Dakota Democrats Ran A Misleading Facebook Ad Discouraging People From Voting," *Buzzfeed News*, Nov. 2, 2018, buzzfeednews.com/article/janelytvynenko/north-dakota-democrats-facebook-ad-voter-suppression

[450] Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About the Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[451] "Soros not owner of company that assembles voting machines," *Associated Press*, Nov. 1, 2018, apnews.com/afs:Content:2457814425
[452] Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About the Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[453] *See* Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About the Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[454] "Are 16 States Using Voting Machines from a 'Soros-Controlled Company'?," Snopes, accessed Feb. 26, 2019, snopes.com/fact-check/george-soros-controls-smartmatic-voting-machines-in-16-states/
[455] "Obama Sold Vote Processing Rights to SCYTL?," Snopes, accessed Feb. 26, 2019, snopes.com/fact-check/scytl/
[456] Jane Lytvynenko, "Election Officials Asked Twitter To Remove a Video Falsely Claiming Voter Fraud, But The Company Refuses," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/janelytvynenko/elections-officials-asked-twitter-to-remove-a-video-falsely
[457] Jane Lytvynenko, "Election Officials Asked Twitter To Remove a Video Falsely Claiming Voter Fraud, But The Company Refuses," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/janelytvynenko/elections-officials-asked-twitter-to-remove-a-video-falsely
[458] Jane Lytvynenko, "Election Officials Asked Twitter To Remove a Video Falsely Claiming Voter Fraud, But The Company Refuses," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/janelytvynenko/elections-officials-asked-twitter-to-remove-a-video-falsely
[459] WWG1WGA (@findtruthQ), "More voter fraud in Ohio. Why is it that all the errors are always the Democrats??," Twitter, Nov. 6, 2018, archive.fo/MFVwx
[460] Jane Lytvynenko, "Election Officials Asked Twitter To Remove a Video Falsely Claiming Voter Fraud, But The Company Refuses," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/janelytvynenko/elections-officials-asked-twitter-to-remove-a-video-falsely
[461] Jane Lytvynenko, "Election Officials Asked Twitter To Remove a Video Falsely Claiming Voter Fraud, But The Company Refuses," *Buzzfeed News*, Nov. 7, 2018, buzzfeednews.com/article/janelytvynenko/elections-officials-asked-twitter-to-remove-a-video-falsely
[462] Jane Lytvynenko and Craig Silverman, "Here's A Running List Of Hoaxes And Misleading Information About the Midterm Elections," *Buzzfeed News*, Oct. 31, 2018, buzzfeednews.com/article/janelytvynenko/midterms-fake-news-hoaxes
[463] Craig Silverman, "A False Claim About 'Illegals' Being Paid To Vote For Beto Originated From A Best-Selling Author And Historian," *Buzzfeed News*, Nov. 6, 2018, buzzfeednews.com/article/craigsilverman/conservative-larry-schweikart-false-claim-beto-illegals
[464] Craig Silverman, "A False Claim About 'Illegals' Being Paid To Vote For Beto Originated From A Best-Selling Author And Historian," *Buzzfeed News*, Nov. 6, 2018, buzzfeednews.com/article/craigsilverman/conservative-larry-schweikart-false-claim-beto-illegals
[465] Craig Silverman, "A False Claim About 'Illegals' Being Paid To Vote For Beto Originated From A Best-Selling Author And Historian," *Buzzfeed News*, Nov. 6, 2018, buzzfeednews.com/article/craigsilverman/conservative-larry-schweikart-false-claim-beto-illegals
[466] Daniel R. Coats, "Worldwide Threat Assessment Of The US Intelligence Community," Senate Select Committee on Intelligence, Jan. 29, 2019, dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
[467] Natasha Korecki, "'Sustained and ongoing' disinformation assault targets Dem presidential candidates," *Politico*, Feb. 20, 2019, politico.com/story/2019/02/20/2020-candidates-social-media-attack-1176018
[468] Natasha Korecki, "'Sustained and ongoing' disinformation assault targets Dem presidential candidates," *Politico*, Feb. 20, 2019, politico.com/story/2019/02/20/2020-candidates-social-media-attack-1176018; "VoterFraud," Guardians.ai, accessed Feb. 26, 2019, iwr.ai/voterfraud/index.html#top
[469] Natasha Korecki, "'Sustained and ongoing' disinformation assault targets Dem presidential candidates," *Politico*, Feb. 20, 2019, politico.com/story/2019/02/20/2020-candidates-social-media-attack-1176018
[470] Alicia Shepard et. al, "Faking News: Fraudulent News and the Fight for Truth," PEN America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf (page 17)
[471] "Democrats used Russian tactics in Alabama. Now they must swear them off.," *The Washington Post*, Dec. 27, 2018, washingtonpost.com/opinions/democrats-used-russian-tactics-in-alabama-now-they-must-swear-them-off/2018/12/27/5b97c332-0941-11e9-a3f0-71c95106d96a_story.html
[472] "Democracy requires authentic discourse," Authentic Elections, accessed Feb. 26, 2019, authenticelections.org/; Justin Hendrix, "Can American Political Candidates Help Stop the Flood of

Disinformation with a Pledge?," Just Security, Jan. 31, 2019, justsecurity.org/62432/american-political-candidates-stop-flood-disinformation-pledge/

[473] "News Consumers' Bill of Rights and Responsibilities," Pen America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/10/PEN_America_Consumer_Rights.pdf

[474] See: "News Consumers' Bill of Rights and Responsibilities," Pen America, Oct. 12, 2017, pen.org/wp-content/uploads/2017/10/PEN_America_Consumer_Rights.pdf