Facebook’s Role in US Elections and
Legal and Technological Approaches Towards Reform

Elaine Hou

May 3, 2018

Advisor: Prof. Joan Feigenbaum, Dept. of Computer Science, Yale University

Abstract

We examine the role that the social media platform Facebook played in the 2016 US presidential election. We first detail how Facebook’s data policies contributed to Cambridge Analytica’s illegitimate acquisition of Facebook user data, which benefited the Trump campaign. Then, we discuss how Facebook’s platform was used by Russian agents in a cyber election interference operation to wage a misinformation campaign on US voters. We contend that international and national governmental organizations failed to enact significant legal countermeasures to combat attacks on US election integrity. Following this is a critique of the technological policy hurdles that hinder Facebook’s attempts to address its negative role in the 2016 election. Finally, we offer propositions for countermeasures for our legal organizations and technological companies.

1 Introduction

On November 8, 2016, the US experienced a major upset in its presidential election. Despite being considered a favorite by a variety of polling organizations and media outlets, Democratic candidate Hillary Clinton lost to Republican candidate Donald Trump [Silver, 2016]. The results were close and contentious; even though Trump won the Electoral College, he failed to win a plurality of votes. The election cycle had been inundated by allegations of Russian cyber election interference in favor of Donald Trump.

Cyber election interference is the use of cyber operations for the purpose of influencing a nation’s elections. It is by no means a new phenomenon, nor is it unique to the US. Some more traditional forms of cyber election interference are cyberespionage, information theft, selective dissemination of information, and breaches of voter registration systems. Some recent examples
of election interference are information leaks of Emmanuel Macron’s campaign in the 2017 French elections and the denial-of-service attacks on Russian opposition leader Garry Kasparov’s website [van de Velde, 2017]. In addition to these forms of interference, information warfare, the creation and dissemination of misinformation, took place during the 2016 election. Although information warfare is also not new, it becomes more pernicious as it becomes easier to spread information.

Enter Facebook. Even before the 2016 US presidential election, Facebook, a social media titan with two billion active monthly users, was a significant political force. In 2012, researchers found evidence that a particular feature the social media website had implemented for Election Day - an "I Voted" button - produced a small yet measurable increase in voter turnout among young people [Madrigal, 2017b]. Since young voters tend to skew Democratic, Facebook’s seemingly innocuous, nonpartisan button may have helped Democratic incumbent Barack Obama win reelection. In a similar situation, Facebook influenced the outcome of a vote on a Republican-leaning measure in the state of Florida. Digital advertising company Chong and Koster used Facebook ads to target two heavily Democratic counties, Broward County and Dade County. Researchers found that Facebook users who were exposed to such ads were 17% more likely to vote in accordance with the ads. This relatively small, highly targeted ad campaign achieved resounding success; despite running ads in only two counties, the measure was defeated [Madrigal, 2017b]. Evidently, Facebook has the capacity to sway and alter elections. Even more importantly, Facebook and other online social media platforms have transformed the ways campaigns and the public interact with each other.

Shortly after the 2016 elections, the public became aware that Russian agents had used Facebook to spread fake news. The social media company immediately came under scrutiny. Facebook CEO Mark Zuckerberg initially tried to minimize its effect, saying that “the idea that fake news on Facebook, which is a very small amount of the content, influenced the election in any way...is a crazy idea” [Mozer and Scott, 2017]. He later expressed regret towards his flippant response. Facebook, along with Google and Twitter, are currently under investigation by Congress for their roles in facilitating foreign election interference [Isaac and Wakabayashi, 2017]. Facebook soon found itself embroiled in another scandal; in March 2018, it was discovered that Trump campaign data consultant Cambridge Analytica had illegitimately acquired the Facebook data of millions of Facebook users for campaign purposes. Facebook clearly blundered in its role in the 2016 election.

It is critical that we consider the ramifications of our social networks on our elections. As it is, Facebook creates opportunities for others to threaten the integrity of our elections. It facilitates information warfare, which sows distrust of the media and of the election process in our citizens. Similarly, if voters believe a campaign can easily infringe on voters’ right to data privacy for electoral gain, the electorate learns to distrust campaigns. If citizen confidence in the democratic process
is undermined, citizens can no longer meaningfully participate in the process, which ultimately threatens the democracy [van de Velde, 2017]. In order to uphold election integrity, we must understand how our modern technological systems, namely our social media and social networks, interact with elections, campaigns, and the political environment.

We proceed as follows. In Section 2, we discuss how Facebook’s lax data privacy policies allowed Cambridge Analytica to acquire Facebook user data. In Section 3, we examine the role Facebook played in the dissemination of misinformation. In Section 4, we address the shortcomings of legal countermeasures against cyber information campaigns instigated for the purpose of election interference. In Section 5, we critique technological countermeasures Facebook has enacted in response to the election. Finally, in Section 6, we provide parting thoughts on the burgeoning role of Facebook in future election cycles.

2 Facebook: Easily Exploitable Data Source

Following Trump’s surprising victory, his campaign’s data consultant, Cambridge Analytica, was hailed for its ingenious data analytics. Cambridge Analytica is a British data consulting firm. It is an offshoot of British political consulting firm Strategic Communications Lab (SCL) Group. Cambridge Analytica has ties to prominent Republican figures. It is partially owned and funded by American hedge-fund manager Robert Mercer and his daughter Rebekah Mercer, both of whom support politically conservative causes, and its former vice president is Stephen K. Bannon, right-wing American media executive and advisor to the Trump campaign. Prior to its work on the Trump campaign, Cambridge Analytica conducted data analytics for the Leave campaign regarding the United Kingdom’s referendum on leaving the European Union as well as for Republican presidential candidate Ted Cruz’s campaign.

One of Cambridge Analytica’s specialties is voter profiling. In 2014, Cambridge Analytica secured a $15 million investment from Robert Mercer and attracted the interest of Steve Bannon with its promise of voter profiling techniques [Rosenberg et al., 2018a]. The concept for voter profiling originated from a Cambridge University Psychometrics Centre study. The study developed a technique for analyzing people’s personalities based on their answers to a personality quiz and information from their Facebook profiles [Rosenberg et al., 2018a]. At a German digital advertising conference, Cambridge Analytica digital director Molly Schweickert explained that the firm’s models use a similar technique of analyzing people’s online activity to generate personality profiles. Specifically, Cambridge Analytica measures a person’s openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism [Illing, 2018]. Personality profiles are useful since they can classify people on characteristics beyond party affiliation and demographic data. Armed
with these voter profiles, Cambridge Analytica can more effectively target political ads towards the most receptive people. Furthermore, should Cambridge Analytica detect an uptick in interest in a particular geographic region, it can alter Trump’s campaign schedule in order to capitalize on local sentiment [Kirchgaessner, 2017]. Under the Electoral College, where a few thousand votes in the right states can sway an election, effective, precise targeting is necessary for campaign success.

Of course, Cambridge Analytica’s models are useless without data. According to Schweickert, these models were based on the firm’s database of voter information and voter surveys. Traditional analytics firms usually acquire data about voting records and purchase histories from public sources or data brokers [Rosenberg et al., 2018a]. Cambridge Analytica also collaborated with political news website Politico to gather data and target an ad about the Clinton Foundation. Most notably, it collected public data from states and counties about early voting and cross-referenced early voters against public information from their Facebook profiles. All of the described information is publicly available in the US [Kirchgaessner, 2017]. These particular sorts of information do not have the predictive power to determine people’s personality traits [Rosenberg et al., 2018a]. Nevertheless, Cambridge Analytica alleged that it had only used legally acquired data for its models.

In March 2018, it was discovered that, on the contrary, Cambridge Analytica had illegally acquired data from over 50 million Facebook profiles [Rosenberg et al., 2018a]. As of April 2018, that number has grown to 87 million [bbc, 2018]. In 2014, Cambridge Analytica employee Christopher Wylie collaborated with former Cambridge University psychology researcher Aleksandr Kogan. They formulated an agreement in which Kogan would collect Facebook profile data for Cambridge Analytica. In return, Cambridge Analytica would allow Kogan to keep a copy of the data for his research and would cover the costs of collecting data, about $800,000. Kogan acquired the data by building a Facebook app, thisismydigitallife. After a person used the app, the app scraped private data from the user’s profile as well as from the profiles of the user’s friends, even if the friends themselves did not consent to having their data harvested. Thus, even though 305,000 individuals gave the app permission to collect their data, the app successfully acquired the data of millions of Facebook users [Granville, 2018]. At the time, Facebook allowed information-harvesting apps to scrape data from a user’s friends without first asking for permission. Once Kogan collected the data, he transmitted the Facebook profile data to Cambridge Analytica [Rosenberg et al., 2018a]. Although Facebook’s policies allow researchers to collect users’ private data, the policies prohibit selling or transferring data to ad networks, data brokers, or other monetization-related services. Kogan’s transferring of Facebook data to a political consulting firm constitutes a violation of this policy [Granville, 2018].

Cambridge Analytica has since acknowledged that it wrongfully acquired Facebook’s data. The firm blames Kogan for violating the social media giant’s policies and claims to have deleted the
data once they realized the illegal means used to collect the data. Meanwhile, in 2015, Facebook updated its policies so as to prohibit apps from collecting a user's friends' data without consent. Along with this change, Facebook removed Kogan's no longer admissible app [Granville, 2018]. Still, at this point, Cambridge Analytica had already acquired the data that would shape the Trump campaign's advertising strategy, travel schedule, and ultimate trajectory.

While Cambridge Analytica undoubtedly deserves public outrage for its dubious acquisition and usage of private information, we cannot ignore Facebook's role in the breach of over 87 million user profiles. Facebook made it possible for researchers to collect a user's friends' private data without permission. Moreover, Facebook did not confirm Kogan's data collection purposes, nor did it implement methods of protecting users' data from being leaked to monetization-related firms. Its privacy policy regarding friends' data was weak, and its implementation of the former policy was even weaker. Facebook's lenient data regulations and lack of foresight rendered it an easy target of exploitation.

3 Facebook: Fake News Medium

During the 2016 election, there were concerns that Russia would meddle with the electoral process. Indeed, the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and National Security Agency (NSA) all concluded that Russian president Vladimir Putin ordered the hacking of Democratic targets with the intent of damaging Clinton's campaign [Shane and Goel, 2017]. The extent of the Russian interference was only made public after the election. Facebook divulged that Russian agents had used its social network to propagate misinformation. Specifically, the Internet Research Agency (IRA), a Russian company that uses online tactics to influence public opinion on behalf of Russian interests, had purchased $100,000 worth of ads on Facebook. About 3000 political ads were found to have links to Russian accounts [Shane and Goel, 2017]. Even more worrisome was evidence that Russian-controlled accounts generated a bounty of controversial and misleading content, colloquially referred to as "fake news" [Albright, 2017]. As of April 2018, Facebook estimates that Russian operatives generated 80,000 Facebook posts [Press, 2018].

For a major US election, Russian activity on Facebook seems insignificant. Most notably, $100,000 is a meager amount. In comparison, in 2015 and 2016, all of the US political campaigns directly bought a total of $11 billion in Facebook ads. Since campaigns may have hired political consultants who, in turn, also purchased Facebook advertisements, $11 billion is, at best, an underestimate [Madrigal, 2017a]. Facebook discovered the $100,000 worth of ads by searching through a subset of all political ads and focusing on those funded by the IRA, so it is possible that there were many more Russian-sponsored ads on Facebook that Facebook has not yet discovered or divulged.
Madrigal, 2017a]. Nonetheless, there is currently little evidence that the amount of Russian political interference on Facebook was comparable to the amount of influence the campaigns garnered on Facebook and other communication platforms.

Considering the relatively small scale of Russian political advertising on Facebook, we cannot assume that the Russian information campaign was intended to sway the election. There are other possible motivations. For instance, the content may have been used as a message-testing protocol. Another possibility is that the misinformation was intended to sow distrust in Facebook’s capacity as a reliable news source. This maneuver could diminish US citizens’ trust in the social media website and in the news media in general [Madrigal, 2017a]. Even without creating enough misinformation to alter voting patterns significantly, Russian information campaigns could have polarized the public and discredited the US electoral system.

Nevertheless, we cannot dismiss the possibility that Russian activity on Facebook was intended to sway the election. Facebook, after all, is a social network; its purpose is to facilitate the sharing of news and stories. Research about the spread of influence through social networks shows that one can influence an entire group to adopt an idea by targeting a specific subset of the group. Although choosing the optimal subset of nodes in the network is NP-hard, a natural greedy algorithm for subset selection can achieve 63% of the optimal case [Kempe et al., 2003]. More specific research about Facebook’s social networks indicates that most information diffusion can be attributed to weak ties, which constitute the majority of connections on Facebook. Facebook and other online social media lower the cost of sharing information, which fosters an environment where weak social ties play a more dominant role. This is in contrast with the real world, where strong social ties have a greater impact on influence [Bakshy et al., 2012]. In short, Facebook creates an environment that can magnify the impact of an information campaign.

Facebook is a particularly expedient medium for spreading misinformation because of its unique news distribution algorithms. For each user, Facebook generates a News Feed, a personalized list of stories and posts that is ranked to maximize user engagement with the platform. The algorithms predict which stories will capture people’s interest through a machine-learning system that examines two thousand features. If the Russian trolls created highly engaging content, such as controversial pages or sensational fake news, their content would be ranked highly by the algorithm. They could then reach millions of Facebook users [Madrigal, 2017a].

The News Feed algorithm itself is proprietary, and Facebook personalizes the content that each individual sees, so it is difficult to measure the spread of Russian-linked Facebook content. Nevertheless, we can estimate the range of its dissemination. According to a Facebook ad specialist, $100,000 worth of ads could reach about between 23 to 70 million people [Madrigal, 2017a]. Research director of the Tow Center for Digital Journalism at Columbia University Jonathan Albright
examined six of the 470 pages that Facebook linked to Russian operatives. He found that those six pages alone had generated 340 million shared posts [Albright, 2017]. In late 2017, it was estimated that Russian influence reached 126 million Facebook users [Isaac and Wakabayashi, 2017]. As of April 2018, that number is now estimated to be 146 million [Press, 2018].

With the prevalence of fake news on social media, it is imperative to examine the nature of its content and its effect on the 2016 election outcomes. Political misinformation and its diffusion heavily favored Trump. A study found that 115 pro-Trump fake stories on Facebook were shared a total of 30 million times, as opposed to 41 pro-Clinton fake stories, which were shared a total of 7.6 million times [Allcott and Gentzkow, 2017]. If we assume that the average US adult saw one fake news story and that one fake story is equally effective at changing vote shares as one television campaign ad, we estimate that fake news swayed the election towards Trump by 0.02% [Allcott and Gentzkow, 2017]. This amount is significantly less than the margin by which Trump won in pivotal states, which initially suggests that fake news had little impact on the results. On the other hand, it is difficult to estimate accurately the true influence of fake news on the electorate. Due to its often sensational and surprising content, false stories could have more sway over individual voters and engage broader audiences. Alternatively, misinformation may have had less influence on the election if it were primarily consumed by citizens who were predisposed to vote a certain way [Allcott and Gentzkow, 2017].

Whether fake news is of foreign or domestic origin and whether it changed the outcome of the 2016 US election, it is important to address Facebook’s role in news distribution and political engagement. Although only 14% of US adults consider Facebook their primary source of election coverage, 62% of US adults acquire information on the news from the social media site [Allcott and Gentzkow, 2017]. Online social media is particularly heinous in circulating falsehoods and bringing fake news websites to prominence. Mainstream news sites receive a small fraction of referrals from social media, whereas fake news websites obtain a larger proportion of their audience from social media [Allcott and Gentzkow, 2017]. From a theoretical and economic perspective, greater amounts of misinformation diminishes the value of all news, thereby obstructing the path towards a well-informed citizenry. Facebook, by giving misinformation a louder voice, has the potential to destabilize our democratic republic.

4 Legal Countermeasures

In light of the negative impact Facebook had on the 2016 US electoral process, we naturally ask what legal countermeasures the US government and other governing bodies had prepared for such circumstances. A legal countermeasure, in this case, refers to actions executed by governments
or organizing bodies for the purposes of upholding the integrity of the democratic process. A fundamental issue in the development of legal countermeasures is that legal jurisdiction often lags behind modern realities. We do not recognize the need for countermeasures until an event has already occurred. Ideally, our legal institutions would take proactive measures against upcoming or potential threats towards election integrity. Unfortunately, political interests and inertia hamper such legal progress.

The 2016 election displays a startling dynamic in which legal action was obstructed by conflicting interests. In the summer of 2016, British private investigator and former intelligence officer Christopher Steele provided the FBI and the US State Department with a dossier about Russian plans to disrupt the 2016 US presidential election via cyber interference. The dossier also accused the Trump campaign of colluding with Russia. Steele expected former President Obama to warn the US about the interference and to threaten Putin with cyberattacks. To Steele’s surprise, the US government reacted very little to his troubling findings. Because the Obama Administration feared provoking cyberwarfare and appearing overly biased in favor of Clinton, the government did nothing. In September 2016, Obama attempted to issue a bipartisan statement addressing Russian election interference, but Republican Senate Majority Leader Mitch McConnell refused to sign the statement. And overall, since people believed Hillary Clinton would win, they felt no urgency to condemn Russian meddling [Mayer, 2018]. The series of events leading up to the 2016 election reveal that inertia and partisanship hindered efforts to protect our election processes.

We address legal countermeasures in two areas where Facebook and US elections interact with one another. First, we ask how legal approaches can protect Facebook users’ data from political exploitation. We then consider how legal jurisdiction applies to cyber election interference conducted via Facebook.

4.1 Legal Approaches to Data Privacy

Facebook’s scandal regarding Cambridge Analytica reveals gaps in US technological policy. Notably, the US, unlike some of its European counterparts, only possesses patchwork data privacy policies. The US has laws, such as HIPAA (Health Insurance Portability and Accountability Act of 1996) and the Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), that protect healthcare privacy and financial data privacy, respectively. However, US companies in other businesses, such as social media and social networking, are mostly self-policing, much to the detriment of their consumers [Gustke, 2013].

In the US, the Federal Trade Commission (FTC) is the government agency responsible for consumer protection; the FTC is currently investigating Facebook for its role in Cambridge Analytica’s breach of Facebook data. In 2011, Facebook signed a consent order with the FTC, in
which Facebook agreed not to misrepresent issues of data privacy and security, to give notice to users in case their nonpublic information is used, and to create a comprehensive data privacy program [Hajjar, 2018]. The FTC has the power to investigate Facebook and can demand more transparency, but it is ultimately unclear whether Facebook violated the consent order. Without more stringent US regulations, Facebook and other social media companies are free to operate with their meager regard for data privacy.

Surprisingly, the most expedient upcoming policy reform that may expand US data privacy rights comes from across the Atlantic. On May 25, 2018, the European Union (EU) will enforce the General Data Protection Regulation (GDPR) [eug, 2016]. This policy updates and strengthens data privacy rights of EU citizens on three fronts. First, GDPR will extend data regulations to all companies that process the personal data of EU residents, even those companies that are not located in the EU. Furthermore, companies in violation of GDPR will be fined up to 4% of their annual global revenue or €20 million, whichever is greater. Finally, the conditions for consenting to allow one’s data to be processed must be stated in clear and plain language, and withdrawing consent must be as easy as giving it. Through the severe penalty as well as the EU’s history of imposing heavy fines on companies that violate data privacy regulations, GDPR acts as an effective deterrent against negligent company data policies. Facebook, with its millions of EU users, must rectify its management of EU data.

The GDPR may compel Facebook to revise how it handles all user data, including the data of US residents. In a hearing before the House Committee on Commerce and Energy, Mark Zuckerberg was asked how GDPR would influence Americans. At first, Zuckerberg stated that Americans would receive the same data protections that Europeans would under GDPR. When legislators asked about ensuring GDPR rights for Americans, Zuckerberg offered an equivocal answer [Jeong, 2018]. It is unclear what provisions of a GDPR-abiding Facebook will be included in the US version of the social platform. As of now, though, without US-driven legal policy, US social media users are subject to the data policy whims of their social media companies.

We ultimately propose that US legislators create a US version of the GDPR. This legislation should require companies to give their users clear, easy ways to manage their data privacy. Furthermore, we should have frequent oversight of companies’ data privacy implementations. Failures to comply with this regulation should be made public and should incur large fines. Our proposition does not outright prevent data breaches, but it would encourage businesses to consider their consumers’ rights.
4.2 Legal Approaches to Cyber Election Interference

From a legal perspective, we struggle to find proper responses to cyber election interference. Cyber election interference refers to actions taken for the purpose of influencing another nation’s elections. Since many instances of election interference happen between nations, we may look to international law for guidance. However, it is unclear and hotly contested what constitutes a proportional response to foreign interference. There is controversy over how the US should respond to Russia’s interference in the 2016 election. Some scholars argue that the US is justified in launching a cyberattack or even a physical attack, and others claim than the US’s options are limited since Russian hacking is an instance of espionage, which the US could only address through criminal law. Still, a third group contends that information campaigns are a hybrid of espionage and outright warfare. They believe that the US can retaliate through cyberattacks. Russia takes the view that its interference in US elections is justified, noting that the US has also frequently disrupted other nations’ political affairs [van de Velde, 2017].

International law is currently ineffective at guiding nations’ responses to election interference. Election interference, particularly cyber election interference, spans a broad swath of activities, from hacking voter registration systems to spreading misinformation. Many international documents only address some forms of election interference, and few address the forms of election interference made possible by technological innovation, such as misinformation campaigns. For example, we would expect the United Nations (UN) Charter to provide guidelines for how a nation should respond to election interference. The UN, in the interest of deterring warfare, sets a high standard for when a sovereign state can go to war. That high standard usually requires that the aggressor state inflicts physical destruction before the victim state is justified in going to war [van de Velde, 2017]. Most cyberattacks do not meet that standard, so the UN Charter offers few means of proper retaliation.

In search of better guidelines, some legal experts choose to interpret other international legal documents more broadly. They invoke the Draft Articles on State Responsibility to justify retribution against aggressor states. There are two types of violations caused by election interference that would justify countermeasures. One is the violation of the norm of non-intervention, which forbids one state from interfering in the domestic or foreign affairs of other states. This definition is too broad - some forms of interference, such as the work of non-governmental organizations in election monitoring, are lawful and should not justify the use of countermeasures. The other is the violation of sovereignty, by which the International Court of Justice (ICJ) refers to a state’s sovereignty over its physical territory. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations expands the definition of sovereignty to cyberspace, but it overextends the notion by saying that states have sovereignty in some circumstances in cyberspace [van de Velde, 2017].
Ideally, we would have effective, contemporary international doctrine regarding cyber election interference. In order to reach such a goal, we must first establish precise and reasonable definitions for election interference, illegal interference, and sovereignty, as they relate to cyberspace. Only then can we aspire to develop useful countermeasures against election interference.

Since international law fails to protect nations from cyber election interference and information campaigns, nations are compelled to address the problem of misinformation themselves. In Chad and Uganda, politicians shut down social media websites ahead of elections. German Chancellor Angela Merkel has called for social media companies to publish their news ranking algorithms to provide greater transparency to voters [Mozer and Scott, 2017]. These responses would not be effective in the US. Many other nations’ solutions involve curbing free speech. Although social media companies have the right to moderate content on their platforms, doing so would violate the US cultural norm of free speech. Demanding more transparency from our social media companies would be logistically unwieldy. First of all, companies alter their algorithms regularly to improve their performance. Keeping the public up-to-date on the algorithms would be excessively difficult. More importantly, many social media algorithms, such as Facebook’s News Feed algorithm, uses machine learning. Explaining how algorithms use machine learning, which itself is an arduous task, would very likely offer no insight on how to combat misinformation.

US legislators have posed several partial methods of responding to Russian cyber election interference. One response has been economic - the Trump Administration has imposed sanctions against Russian oligarchs and their associated companies [Borak, 2018]. Another way of confronting cyber election interference is to require greater transparency from our social networks. In October 2017, Senators Amy Klobuchar and Mark Warner introduced the Honest Ads Act, a bill that would require Internet companies to identify those who paid for political ads on their platforms [Isaac and Wakabayashi, 2017]. The Honest Ads Act has recently gained attention following Facebook’s endorsement of the bill [Nieuva, 2018]. Currently, it is unclear whether the bill will pass.

The US has a long way to go to combat cyber election interference effectively. Russia is unlikely to be deterred by sanctions; Konstantin Kosachev, one of the Russian oligarchs targeted by the sanctions, said the following in response to the sanctions: “This is an attempt to use the sanctions to justify the absence of a real strategy and justify the alleged legitimacy of its actions against Russia. This is the way to nowhere. Russia cannot be frightened by it and especially cannot be broken by it” [Borak, 2018]. Furthermore, even if a bill regulating online political ads were to pass, foreign agents could still somewhat obscure their identities. This bill also does not counter the proliferation of Russian-linked Facebook pages, which are allowed to post controversial or false content. Under our nation’s current legal system, individuals are generally allowed to create and circulate misinformation.
Our current legal responses are inadequate since they address the side effects of information campaigns instead of seeking preventative measures. We must counter the symptoms as well as the causes of cyber election interference. We propose a stronger response to cyber election interference, one echoed by Christopher Steele: we must make the public aware of the threat, and we must construct clear, meaningful consequences against violations of our election integrity.

5 Technological Countermeasures

Technological countermeasures refer to the technological changes implemented in response to election interference. They are ultimately software or hardware alterations, but such changes arise from a reform in a company’s policy and philosophy. Facebook, which has recently undergone government investigation and social judgment, has unveiled a series of modifications to its social media platform. We review the technological changes made in response to the data breach and to misinformation, and then we examine Facebook’s culture and philosophy.

5.1 Technological Approaches to Data Privacy

In response to the Cambridge Analytica data scandal, Facebook announced several changes to its management of data privacy. Most notably, the company is removing the Partner Categories feature, which permitted a flow of data between Facebook and data brokers, such as Experian and Oracle. Data brokers will now no longer be able to use their own consumer data to target users; they will instead have to use Facebook’s own targeting tools to target consumers. Facebook will also stop providing anonymized data to data brokers about their ad campaigns [Hern, 2018]. By curbing the spread of data to third parties, the social media company hopes to minimize concerns about data privacy.

Its recent changes in data privacy management are expected to have minimal impact. Although it is an improvement, shutting down Partner Categories would not have prevented the Cambridge Analytica scandal, in which the data was leaked by an academic’s app. Facebook claims that the information it shares with third parties is non-personally identifying information; it does not share information such as one’s name or email address [fbd, 2016]. However, according to data privacy research, any attribute can be identifying in combination with other attributes. De-identifying data is a weak form of privacy protection [Narayanan and Shmatikov, 2010]. Senior research analyst at Pivotal Research Group Brian Wieser questions the efficacy of removing Partner Categories on protecting consumers’ data. He instead views the change as Facebook’s attempt to distinguish itself from other major technology corporations [Hern, 2018].

Moreover, Facebook is implementing a centralized system where users can control their data
privacy and security settings. This is a major improvement over the current system of having data privacy settings scattered across twenty different locations on the platform. The privacy center allows users to control the information Facebook has about their political stances and interests, review the data Facebook already has about them, and examine the data collection capacities of the apps they are using [Frenkel and Singer, 2018]. Such a measure would reassure users that their information is secure.

The privacy center consolidates existing privacy features, but it offers limited control over one’s data. According to Facebook’s data policy, the company still collects users’ personal and network data and reserves the right to share sensitive information with apps, websites, and third parties [fb, 2016]. Furthermore, some data privacy experts speculate that Facebook’s granular privacy controls even encourage users to share more data. According to the control paradox, when users believe they have more control over their privacy, they are more willing to share sensitive information [Porter, 2018]. Through its weak data privacy policies and implementations, Facebook demonstrates that it does not highly prioritize user data privacy.

There are changes that Facebook could implement to improve its data privacy protections. One major fix would be to limit the user data Facebook makes available to third parties. Another is to impose harsher penalties on the third parties that abuse such data. The Cambridge Analytica scandal has occurred, but stronger retaliation from Facebook could deter future data breaches. These tactics would prevent some data breaches and demonstrate genuine dedication towards protecting the interests of users.

5.2 Technological Approaches to Cyber Election Interference

Facebook is addressing the issue of the dissemination of misinformation as well, a problem that is difficult to target at its root. Whether or not foreign agents buy political advertising on Facebook, they can still create polarizing content and circulate it on the platform. The initially attractive and straightforward solution of finding and removing Russian-linked content is problematic since it sets a potentially detrimental precedent of suppressing foreign-created content [Isaac and Wakabayashi, 2017]. Hence, Facebook cannot prevent the spread of fake news merely by banning it. Facebook is instead taking a two-pronged approach where it verifies users more rigorously, and it minimizes the spread of misinformation.

Verifying the authenticity of Facebook accounts can reduce fake news since foreign agents would be less able to pose as US citizens and residents. For the 2016 election, Facebook banned some Russian agents because they did not identify themselves authentically on the platform, which violates Facebook’s policies [Isaac and Wakabayashi, 2017]. Facebook recently announced that people who want to buy political ads on the website must first verify their identity and location.
Ad-buyers will be required to submit proof of a government-issued identification, and they must have a US mailing address [Nicas, 2018].

However, the social platform has allowed many fake accounts to remain on the website. Harvard Law School professor Jonathan L. Zittrain contends that Facebook and other social media companies allow fake accounts to remain on their platforms since their business models rely on growth [Shane and Isaac, 2017]. Even if Facebook were to remove inauthentic accounts, this would have a marginal effect on the quality of the news it spreads. According to Facebook vice president of policy and communications Elliot Schrage, the content of Russian agents’ pages did not violate Facebook’s policies and would have been allowed on the website had individuals operating the pages represented themselves authentically to Facebook [Isaac and Wakabayashi, 2017]. The recent push for political ads from verified people is not foolproof - with some effort, foreign agents could still masquerade as US citizens and circulate misinformation. Better account verification on Facebook is necessary for combating election interference, but it is by no means sufficient.

Facebook is also attempting to stymie the spread of misinformation on its platform. Facebook’s fake news situation differs from that of other platforms, such as Twitter; whereas bots are widely used on Twitter to disseminate falsehoods, people are the primary distributors of news on Facebook [Wong, 2017]. Facebook has recently overhauled its News Feed algorithms, a development that can be interpreted as a countermeasure to fake news. Specifically, the social media site intends to prioritize content from friends and family and to deemphasize content from publishers. Zuckerberg attributes the planned changes as a means of fostering more meaningful interactions [Isaac, 2018]. People would hear less from publishers, which could reduce the reach of fake news. Facebook will also introduce a system for ranking the veracity of news sources. After asking users to rate the trustworthiness of news sources, Facebook will prioritize the most trusted sources in users’ News Feeds. This modification will be in place until at least the 2018 US midterm elections [Seetharaman, 2018].

Facebook’s actions towards improving the content of News Feed are marginal countermeasures at best. Fake news could still spread if a friend or relative shared misinformation. Also, by ranking friends’ and relatives’ posts more highly, Facebook risks categorizing people into social bubbles instead of cultivating more connections with greater diversity [Isaac, 2018]. While the shift towards trustworthiness scores is well-intentioned, its implementation has the potential to be ineffective. The platform relies on users to rate the trustworthiness of publishers, which does not necessarily guarantee higher-quality news. These changes alone are not enough. Facebook has been testing changes to its algorithms in other nations, with sometimes abysmal results. In 2016, when Facebook tested its News Feed alterations in Slovakia, publishers said that the changes actually helped promote fake news [Frankel et al., 2018]. Facebook simply cannot guarantee that
its stated changes will improve the platform.

Facebook is in the process of implementing many features to reduce fake news, but it is unclear whether any technological solutions could be effective. Its current and proposed measures for authenticating users can be sidestepped. In some cases, Facebook’s attempts at solving the problem of misinformation have backfired. Even if Facebook could implement artificial intelligence that could identify and block fake news, malicious agents could engineer fake news that bypasses Facebook’s filters. Even though Facebook ought to develop these tools, the company cannot and should not expect these tools to be effective for long.

5.3 Technological Approaches and Facebook’s Culture

Facebook has announced many changes to its platform in the name of improving its role in elections. Yet at its heart, Facebook is not truly reforming its services. The company’s decision not to pursue more drastic reform stems from its culture of self-interest.

From an economic standpoint, social media outlets like Facebook benefit from growth. As it gains more users, Facebook generates more revenue per user. In late 2017, Facebook’s average revenue per user first exceeded $5, and US and Canadian users generate, on average, $21.20 per user [Shinal, 2017]. When its consumers frequently use its services, expose themselves to ads, and provide more data, Facebook generates more revenue as well. Controversial and inflammatory discourse and misinformation drive participation, which generates more profit and social capital for Facebook [Rainie et al., 2017]. If anything, successfully combating fake news would negatively influence Facebook’s bottom line.

There is also evidence that Facebook leaders and employees prioritize their company’s growth. In a 2016 Facebook internal memo, Vice President Andrew Bosworth presents the argument that Facebook must prioritize growth tactics above all else for the sake of connecting people [Mac et al., 2018]. When this memo was leaked to the public in 2018, Zuckerberg publicly disavowed with the memo, and Bosworth himself stated that he disagreed with the memo back when he wrote it as well as now [Mac et al., 2018]. However, Bosworth asserts he wrote the memo to expose issues with the company’s philosophy; this itself is evidence that some people at Facebook value growth at the cost of negative externalities.

Another issue with Facebook’s creed is that its community standards limit how it can handle misinformation. According to Facebook’s Community Standards, since Facebook ultimately does not want to stifle public discourse, which includes satire and opinions, Facebook does not remove false news; it attempts to reduce the distribution of false news by placing it lower in News Feeds [fbc, 2018]. With Facebook’s current policies, false content creators can still find ways of manipulating the platform to spread falsehoods. Foreign agents, such as Russian agencies, can sidestep
Facebook’s policies and continue to wage information campaigns.

To its credit, Facebook has, on the surface, shown interest in playing a positive role in society and in fostering public engagement. At its core, though, Facebook’s underlying motivations sometimes conflict with the public interest of having fair and genuine elections. Naturally, we cannot depend on Facebook to address all of the problems regarding its role in the 2016 election unilaterally. In the words of Senator Amy Klobuchar, we cannot rely on a “patchwork of voluntary measures from tech companies” to solve problems surrounding our elections [Nicas, 2018].

6 Facebook and Future Elections

The impact of Facebook on the 2016 US elections offers a unique case study in how apathy from legal and technological bodies can facilitate unintended and unwanted consequences. Our governing organizations and Facebook now contend with the reality that they did not undertake adequate measures to address election issues. Social media platforms - not merely Facebook - have made it easier to undermine election integrity. And the problem is still present - as we approach the 2018 US midterm elections, there are concerns that Russia is again meddling with our elections [Rosenberg et al., 2018b].

We maintain that not all hope is lost. The available countermeasures are vague and relatively weak, and we cannot reasonably expect reform from merely the legal or technological stance to uphold the integrity of our elections. Nonetheless, there are directions we can take that will improve our situation. We advocate a concerted joint effort between our governmental bodies and our technology companies. This solution requires long-term coordination and collaboration as well as introspection on past failures. It is a difficult solution. Despite that, we must pursue change and improvement. After all, it is crucial that we protect our election processes and, with them, our democracy.

Acknowledgments

This work was produced for CPSC 490 in completion of the BS in Computer Science at Yale University. The author would like to thank advisor Prof. Joan Feigenbaum for her insightful advice and continual support. Thank you for giving me the courage and direction to delve into the 2016 US election.

References


[Press, 2018] Press, A. (2018). As many as 146 million people on Facebook may have received information from Russian agency, Zuckerberg says. Public Broadcasting Service. [Online; posted 09-April-2018].


