Executive Summary

The 2016 presidential election in the United States was arguably the event that saw the issue of online disinformation erupt into the public consciousness. Indeed, research subsequently revealed that as many as 65 million Americans visited a disinformation website in the weeks leading up to 2016 election, and the phenomenon of so-called “fake news” was hotly debated both online and off.

In the years since, the role of online disinformation in the 2016 election, and its potential impact on the victory of President Donald Trump, have been the subject of a growing body of empirical research. These studies show that disinformation on social media was indeed widespread. At the same time, most research finds that such disinformation did not influence the outcome of the election, though the broader Russian information warfare campaign may have.

The comparatively early experience of the United States with online disinformation and the subsequent efforts to document and measure its impact—as well as the evolving responses of policymakers, social media platforms, and others—render the U.S. a useful case study for other countries contemplating this challenge. In Latin America, disinformation—false information deliberately and often covertly spread to influence public opinion—has been a feature of recent elections in countries that include Brazil, Colombia, and Mexico. As social media’s relevance as a source of political news expands, so too will the potential reach and impact of disinformation.

For regulators, platforms, and citizen groups working to respond to this challenge, the U.S. experience offers essential insight that argues against both complacency and overreach.

This policy brief, based on publicly available information and a survey of the existing academic literature, summarizes what we know about the role of online disinformation in the most recent U.S. elections and distills relevant policy implications with Latin America in mind. Taken together, the recommendations that we derive from U.S. experience—for governments, technology companies, and civil society—suggest that there is no silver bullet against online disinformation. Instead, disinformation is best addressed via agile, collaborative, multistakeholder responses that combine carefully conceived, rights respecting regulation; technological adaptations by social media platforms; and civil society-driven efforts in areas such as fact-checking and digital literacy.
In June 2018, the democratic nations of the Western Hemisphere gathered for the annual General Assembly of the Organization of American States. Among the issues on the minds of the foreign ministers in attendance was a collective concern regarding the deliberate, online dissemination of disinformation, particularly during electoral periods. In an effort to respond to this emerging concern, the General Assembly approved a resolution mandating the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (“Special Rapporteurship”) to develop recommendations on guaranteeing freedom of expression and access to information from diverse sources, free from undue interference, during electoral periods.

To fulfill the mandate established by OAS Member States, the Special Rapporteurship appointed a panel of experts on disinformation in electoral contexts, which met in Mexico City in April 2019. The panel is comprised of regional experts from civil society, academia, technology companies, think tanks, fact checking organizations, and the media. With the support of the OAS Department of Electoral Cooperation and Mexico's National Electoral Institute, the experts discussed the appropriate conceptual framework for online disinformation, analyzed emblematic case studies, and debated potential regulatory and technological responses to the disinformation challenge within the framework of the Inter-American human rights system's expansive protection of freedom of expression.

To be sure, disinformation in electoral periods is not a new phenomenon. However, social media platforms have introduced a powerful new vector into the equation, raising legitimate concerns about the impact of deliberate, malicious, and widespread disinformation on democratic processes. The spread of disinformation in recent elections across the Americas—from the United States to Brazil, Colombia to Mexico—only served to reinforce these concerns. At the same time, it is crucial that potential responses to disinformation be grounded in human rights law and based on a rigorous analysis of disinformation's scope and impact.

The case study presented in this policy brief focuses on the 2016 elections in the United States. It is a vital case study not just because of the prominence of deliberate disinformation in that election, but also because of the level of empirical research that has since occurred regarding this phenomenon. The study, co-authored by Ben Raderstorf and expert panel member Michael Camilleri, was first presented at the experts’ meeting in Mexico City. It contributed significantly to the group's understanding of disinformation's role in the 2016 elections, and—as importantly—the lessons that can be derived from U.S. experience that may be relevant to the broader region. The report's publication will further this necessary and urgent discussion among relevant stakeholders throughout the Americas.

Online disinformation is a complex challenge that defies easy answers and will require an ongoing commitment to the search for solutions among governments, international organizations, technology companies, and civil society. I commend the Inter-American Dialogue’s thoughtful contribution to this collective endeavor.

EDISON LANZA
Special Rapporteur for Freedom of Expression
Inter-American Commission on Human Rights
Introduction

Fifty-five Savushkina Street in Saint Petersburg, Russia is a four-story, glass and granite, otherwise nondescript office building in a quiet outer neighborhood north of the Neva River.

The building is easily missed. It is also the last-known headquarters of the Internet Research Agency (IRA), the world’s most infamous digital information warfare outlet, often referred to as a “troll farm.” With at least 600 well-paid employees, the organization conducts online disinformation, harassment, hoaxes, and other propaganda operations around the world in coordination with and on behalf of the Russian government.³

According to reporting from the New York Times, the IRA has spent years harassing and attacking the political enemies of Russian President Vladimir Putin both inside and outside Russia.⁴ The organization also creates expansive and coordinated hoaxes and disinformation campaigns.

On September 11, 2014, the organization spammed residents of St. Mary Parish in the U.S. state of Louisiana with fake text message alerts, social media posts, and online videos of a non-existent industrial disaster and toxic chemical link.⁵ The hoax included faked videos, supposed evidence linking the “attack” to ISIS, and social media posts calling for the U.S. to “bomb Iraq”—all timed for the anniversary of the September 11 attacks.⁶

Later that year, it coordinated similar hoaxes, with a supposed outbreak of Ebola in Atlanta and false rumors that a police officer had shot an unarmed black woman, also in Atlanta,⁷ with the hashtag #shockingmurderinatlanta.⁸ Both were clearly designed to tap into two of Americans’ greatest anxieties that year: the West African Ebola outbreak and the spate of police shootings of unarmed black men and women highlighted by the Black Lives Matter movement.

Then came the 2016 election, when the IRA’s operations in the United States shifted from random trolling to war footing. Together with other actors in Russia, the organization was part of a sustained propaganda, disinformation, and hacking campaign. According to the U.S. intelligence community’s 2017 report, “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election, the consistent goals of which were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.”⁹

At the same time, the IRA and other Russian actors were only one part of the explosion of disinformation and other online information manipulation that took place during that election. A swarm of domestic and foreign actors took advantage of the internet to spread falsehoods and sow chaos. While the extent of the implications of the disinformation campaigns is difficult to gauge—much less to comprehend and summarize in any meaningful way—the 2016 election in the United States can be seen as the dawning of a new age of information warfare.
What Happened? Disinformation in the United States

It is no secret that the 2016 presidential election and 2018 congressional election in the United States were both marred, in various ways, by intervention and manipulation online. Multiple U.S. House of Representatives and Senate reports, academic studies, and independent journalistic investigations have all shed light on a sophisticated and multi-faceted disinformation campaign by both foreign and domestic actors.

The scale alone should draw significant attention. A study by Matthew Hindman and Vlad Barash for the Knight Foundation found more than 6.6 million tweets linked to disinformation and conspiracy sites in the month before the 2016 election. One estimate found that more than one-quarter of voting-age adults in the United States visited a disinformation site in the final weeks of the 2016 election. Russia-linked accounts alone reached 126 million people on Facebook and 20 million on Instagram.

The wave may not have crested. One study from Oxford University found that the sheer quantity of "junk news" in U.S. social media actually increased in the 2018 election, as compared to two years prior, "with users sharing more junk news than professional news overall." (That said, other studies find the opposite—that disinformation declined significantly between 2016 and 2018.)

By The Numbers

According to reports prepared for the U.S. Senate and other sources, here are a few facts:

- Between 2013 and 2018, IRA social media campaigns reached tens of millions of Americans and were shared over 30 million times between 2015 and 2017.
- A far larger number—as many as 65 million people—visited a disinformation website not necessarily linked to Russia in the final weeks of the 2016 election.
- IRA campaigns used Twitter, Facebook, Instagram, YouTube, and other platforms and were spread both through advertisements and organic activity.
- Russian disinformation campaigns did not stop after the 2016 election, or even after the U.S. Department of Justice indicted 13 Russian individuals and three companies, including the IRA, in February 2018 for "information warfare against the United States."

Identifying Disinformation

Most disinformation is designed at face value to resemble actual, albeit politically biased, news and commentary.

Especially on the right, disinformation in the United States often resembles various arch-conservative media and opinion sites such as the Drudge Report and Breitbart, which are often speculative and unsourced but not necessarily false. Websites such as the "Conservative Daily Post" circulated fabricated stories about Hillary Clinton promising amnesty for undocumented immigrants in exchange for their votes, or complicated conspiracy theory stories linking the Clinton campaign to a "massive child trafficking and pedophile sex ring." Three days before the 2016 election, a fake online newspaper calling itself "The Denver Guardian" ran a story with the headline "FBI agent suspected in Hillary email leaks found dead in apparent murder-suicide." While they spread on social media, these disinformation outlets have their own sites, many of which are regularly updated with new material.

As many as 65 million people visited a disinformation website in the final weeks of the 2016 election.

In contrast, much of the disinformation linked to Russian operatives tended to be spread specifically through social media ads, pages, groups, and promoted posts. One Instagram ad accused Hillary Clinton of asking "What difference does it make?" over an image of a grieving military widow. Another Facebook ad targeted users with connections to the civil rights movement with a message supposedly from an "out-of-wedlock son of former President Bill Clinton and a black prostitute."

Some efforts focused on voter suppression specifically, including false voting rules (such as claims that one
Defining Disinformation

By nature, “online disinformation” is a slippery and politically loaded term. It is often used interchangeably with terms like misinformation, propaganda, conspiracy theories, lies, deception, and “trolling.” The definitional challenges, however, are not just academic.

Nowhere is this clearer than in the dizzying redefinition of the term “fake news” and its connotations in U.S. politics and around the world. During and after the 2016 U.S. election, the specter of “fake news” exploded across the media and the internet—it was even named the 2017 Collins Dictionary word of the year. The term was initially popular as a criticism of Donald Trump and his supporters’ disregard for facts and evidence, but Trump and other conservative activists quickly appropriated the term as a catch-all attack on the mainstream media. In early 2018, the Republican Party website posted a list of “Fake News Awards.” The top five recipients? Reporters and columnists from The New York Times, ABC News, CNN, TIME, and The Washington Post.

Today, “fake news” is a favorite attack on critics and the independent media by populist and authoritarian leaders around the world.

Disinformation, narrowly defined, is “false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth.”

This brief takes “online disinformation” specifically and narrowly to mean information that is demonstrably false and deliberately spread on the internet with the intention of shaping public opinion. This separates it from “misinformation” which is false information, but that may not be deliberately so. It also avoids the somewhat different connotations of “propaganda” and “deception.”

Disinformation vs. Hacking

It is extremely important to note the difference between disinformation and other types of information warfare, such as hacking and leaks of stolen information. By far the most important example of the latter is the GRU/Wikileaks email hacks of the Democratic National Committee, the Democratic Congressional Campaign Committee, and Hillary Clinton’s campaign chairman John Podesta. Starting in July 2016, the Russian government’s intelligence agency GRU broke into private servers and stole email records from prominent Democrats close to Hillary Clinton. Then, using the whistleblower website WikiLeaks as an intermediary, the GRU selectively leaked embarrassing exchanges over the following months. In doing so, Russia aimed to manipulate the U.S. media into keeping negative stories about Hillary Clinton—and her emails—in the news as much as possible while drawing negative coverage away from Donald Trump.

Arguably, it was these “hack-and-dump” operations that had the largest impact on the outcome of the 2016 election, and may have been pivotal in helping Donald Trump win. The role of these hacks—and potential coordination between the Trump campaign, WikiLeaks, and Russia—was also a prominent focus of Special Counsel Robert Mueller’s investigation.

That said, stealing and releasing documents, even online, should not be confused with disinformation campaigns, which specifically spread false information. While Russia’s information warfare strategy integrated the two—and both contributed to the same generalized confusion and dissension—they should nonetheless be held apart. Disinformation and hacking are fundamentally different operations and require separate policy responses. This brief focuses on disinformation.

could vote by text), messages in support of third-party candidates, and other encouragements for voters to avoid voting for a major party candidate.

Other examples of Russian social media campaigns were not strictly disinformation, but rather mimicked genuine political messages from different groups. One ad targeted Bernie Sanders supporters with a real quote from Sen. Sanders about the Clinton Foundation. One even encouraged members of the LGBT+ community and allies to rally against the Westboro Baptist Church, a far-right hate group. That said, almost all of the content was—either directly or indirectly—connected to promoting Donald Trump and undermining Hillary Clinton.

Blurry Lines Between Foreign and Domestic

Perhaps rightly, much of the focus in the U.S. debate over disinformation has been around Russian actors and foreign
intervention in the country’s elections. To some degree this makes sense: many democratic societies expressly endorse some actions by domestic actors that are strictly forbidden to foreigners, such as donating to campaigns.

That said, although public debate is quick to point the finger at Russian meddling, much of the most pernicious and impactful disinformation originates within the United States.\(^\text{37}\) And all indications suggest that the drive towards disinformation will only grow, on both sides of the aisle. In the 2017 special Senate election in Alabama, Democratic operatives engaged in multiple disinformation schemes aimed at undermining the Republican candidate, Roy Moore.\(^\text{38,39}\) One such scheme presented fake information that Russian Twitter bots were attempting to sway the election, while another falsely alleged that Roy Moore would potentially seek to ban alcohol.\(^\text{40}\) As The New York Times put it, “[r]eality-warping attacks are now coming from inside the house.”\(^\text{41}\)

This hits at the central threat of disinformation: lies and falsehoods are, in theory, a strategy open to all political actors. The only things preventing disinformation are norms and votes. Once efficacy has been proven, the same tactics are almost certain to be emulated by others. To some degree, the very separation of disinformation into online-vs.-off, foreign-vs.-domestic misses the bigger picture: a political discourse rapidly losing its moorings in truth. According to the Washington Post, President Trump made 8,158 false or misleading claims in his first two years in office—more than 11 per day.\(^\text{42}\) In that time, his approval ratings among Republicans never dropped below 80 percent.\(^\text{43}\)

As they respond to disinformation online, governments should avoid the temptation to treat the problem as easily isolated or solved. A culture in which no political holds are barred is, by nature, more susceptible to disinformation. When it comes to political decay, online falsehoods are just as much a symptom of declining norms and accountability as its cause.

Higher Platforms: A Changed Media Landscape and the Role of Social Media

The lion’s share of disinformation during the 2016 election tended to be spread by older voters and via social media.\(^\text{44}\) According to Hunt Allcott and Matthew Gentzkow, disinformation websites gather approximately four times more of their traffic from Facebook, Twitter, Instagram, and other social media sites, as compared to real news outlets.\(^\text{45}\) In fact, the viral potential of disinformation is staggeringly high. According to analysis by Buzzfeed News, the “top fake election news stories generated more total engagement on Facebook than top election stories from 19 major news outlets combined.”\(^\text{46}\) To be sure, engagement does not necessarily measure impact—a majority of accounts linked to disinformation are tightly networked, automated “bots.”\(^\text{47}\) Still, virality on social media is integral to both the spread and impact of disinformation.

Online decentralization is also a major challenge in quantifying and responding to disinformation. Social media platforms—in the United States, that means Facebook, YouTube, Instagram, and Twitter above all—are in many ways the new nexus of political communication. According to the Pew Research Center, in 2016 almost two thirds of Americans got their news, at least in part, via social media.\(^\text{48}\) The good news is that most consumers are skeptical: 57 percent view social media news as “largely inaccurate.”\(^\text{49}\) That said, the socialization of political information flows, in both origin and distribution, means that the marketplace of ideas is harder to monitor and understand. It also makes the very concept of truth harder to reinforce. Without common norms and conduits of information, verifiable information is suddenly at a disadvantage. Unsurprisingly, trust in the media has consistently declined in recent years in the United States.\(^\text{50}\)

This shift also gives enormous power to social media platforms. It is crucial to bear in mind that the internet is in many ways a powerful democratizing tool. Social media platforms in particular help broaden the political debate, open it to traditionally marginalized voices, and facilitate citizen interactions with candidates and elected representatives. At the same time, these platforms are by nature more opaque and harder to regulate than traditional media. Social media presents challenges to the health of
Social media presents challenges—including disinformation—to the health of democratic debate and discourse, some of which are arguably inherent to its business model.

Democratic debate and discourse—including but not limited to online disinformation—some of which are arguably inherent to a business model based on maximizing user engagement to fuel revenue.

In 2015, for example, Twitter shifted from showing tweets in reverse chronological order to an algorithmic newsfeed which partially displays tweets based on a calculation of “relevance” rather than recency. Human biases make us more likely to react to content that taps into existing grievances and beliefs, meaning that inflammatory tweets often generate quick engagement and, as a result, reach more users via the algorithm.

A similar critique has been leveled at YouTube, which introduced a “recommendation” algorithm in 2012 in an effort to keep users on its site. Critics alleged that in an effort to drive usage and achieve its goal of one billion viewing hours per day, YouTube’s algorithm pushed viral misinformation, political extremism, and content offensive to children. YouTube itself acknowledges that when the recommendation feature launched, it optimized for content that got users to click, incentivizing the creation of misleading and sensationalist clickbait.

The internet—especially in a large, diverse, and polarized country like the United States—is ripe ground for disinformation to germinate and spread. As Abby Wood and Ann Ravel describe, disinformation has thrived in an environment of sparse transparency for political advertising and activity online. Unlike advertising and political messaging through traditional broadcast media, the micro-targeted and opaque targeting that takes place on social media has largely avoided any serious regulatory oversight, regardless of source or veracity.

The effect is exacerbated by the substantial financial rewards for creating and disseminating viral content, even and perhaps especially if it is misleading. A 2016 Buzzfeed report published five days before the November 2016 election revealed that Macedonian teenagers were making up to $5,000 a month in ad revenue from Trump-related disinformation sites. While Google and Facebook have both attempted to cut off disinformation sites from placing or profiting from ads, the underlying financial incentive to drive traffic with online falsehoods will never fully disappear.

To be fair, most social media platforms have—perhaps belatedly—sought to respond to disinformation’s spread. While a complete cataloging of these measures is beyond the scope of this report, these measures range from algorithm and advertising policy changes, to enforcement of community standards, to efforts to promote quality journalism and digital literacy. While efforts in the U.S. Congress to mandate transparency in online advertising following the 2016 elections have yet to bear fruit, both Google and Facebook have taken steps to create searchable archives of spending on political ads in the United States. Facebook also changed its algorithms and instituted new features in the wake of the 2016 election.

Initial indicators show that these efforts have worked. A study from NYU and Stanford researchers found that engagements with disinformation on Facebook had fallen by more than 50 percent since the 2016 election. However, as the authors note, “the absolute quantity of interactions with misinformation on both [Facebook and Twitter] remains large, and that Facebook in particular has played an outsized role in the spread of disinformation.”

The scope of the challenge can be daunting. In the third quarter of 2018 alone, Facebook disabled 754 million fake accounts in application of its community standards.

Google and YouTube have also adopted a series of measures to combat disinformation. These fall into three broad categories. First, community guidelines are enforced to remove content that, for example, involves impersonation or the use of automated systems to artificially increase views. Second, ranking algorithms are evolved to elevate high-quality information. YouTube, for example, added a measure of “social responsibility” to its recommendation algorithm in late 2016. It later removed millions of channels for violating its guidelines, began featuring “authoritative” sources from established media outlets in its news sections, and created a new category of “borderline content” that is
Third, affirmative steps are taken to provide context to users via, for example, information panels on YouTube that display additional information and links to authoritative third-party sites. At the same time, technology companies are averse to revealing detailed information about their proprietary algorithms and even their internal guidelines for enforcing community standards, meaning there remains a significant level of opacity about the information that reaches users.

Particularly where content removal is concerned, this opacity is a potential vulnerability, exposing the platforms to criticism over their decisions to effectively censor content with little oversight or accountability. Facebook’s decision to create an Oversight Board for Content Decisions could, if adequately empowered, provide a mechanism to independently review and further elucidate how the company balances engagement and quality of information.


Although disinformation is clearly a threat to democratic discourse, policymakers should also be cautious in over-ascribing it as the central root of modern democratic turmoil. Several studies have cast some degree of doubt on the ability of disinformation to change ideological perspectives and political outcomes. Take, for example, one very influential study by Andrew Guess, Brendan Nyhan, and Jason Reifler, which found that disinformation exposure in the 2016 U.S. election was widespread, but mostly limited to intense partisans whose views were unwavering. According to Nyhan, there is "no association between pro-Trump fake news exposure and differential shifts in candidate support or voter turnout." The researchers also found that disinformation consumption was concentrated among voters older than 60, possibly reflecting a lack of digital literacy.

Another study by R. Kelly Garrett found that while millions of Americans have engaged with inaccurate messages via social media, its use had no measurable aggregate influence on issue beliefs in the 2016 elections and is not a major driver of political misperceptions. In fact, it found that Facebook users had reduced issue misperceptions compared to those who used only other social media.

There are also doubts about whether disinformation, especially when viewed casually on social media, has a lasting impact on voters—beyond cementing preconceived opinions. One study from NYU and Stanford researchers found almost no discernable recall of any specific fake news headline several months after the 2016 election. This fits with existing research that has found political persuasion to be extremely difficult in all contexts. One study, for example, found that exposure to a political ad only shifts the partisan vote preference of 0.02 percent of voters. In other words, there is no clear evidence that disinformation stories are believed, in any lasting or specific way, by a sizeable percentage of voters. More likely, it seems, weaponized political falsehoods are most effective in reinforcing and radicalizing existing and more generalized partisan beliefs and values. That implies that disinformation is only part of a complex ecosystem of growing polarization, ideological entrenchment, and information silos—and should be treated accordingly.

Notwithstanding the abovementioned body of evidence, there is at least one empirical study that argues online disinformation did have a decisive impact on the outcome of the 2016 election. Academics from Ohio State University measured the tendency of voters who supported Barack Obama in 2012 to defect from Democratic candidate Hillary Clinton in 2016 based on whether they believed three widely circulated false news stories alleging that: 1) Hillary Clinton’s health was failing; 2) Clinton approved
weapons sales to Islamic jihadists; and 3) the Pope endorsed Donald Trump. Of Obama voters who did not believe any of the stories, 89 percent voted for Clinton; among those who believed two or three of the stories, only 17 percent voted for Clinton. The researchers argue that, in an election decided by just 78,000 votes in three key states, it is “highly likely” online disinformation influenced the outcome of the election. As always, though, the difficulty is establishing the causal chain—did believing disinformation make defection from Obama to Trump more likely? Or were marginal voters that were more likely to switch to Trump also more likely to believe disinformation? The truth may be some combination of the two.

Conclusion: Disinformation as Chaos and Uncertainty

At the core, disinformation is designed to destabilize. That remains true whether the target is a candidate, a political party, an ideology, a country, or the very idea of democracy.

In fact, the very goal of disinformation—not unlike terrorism—may partially be to provoke panic and an outsized response. While false content is often framed as attacking or supporting a specific party or candidate, the larger goal is to undermine trust in institutions and truth in general. When anything can be true online, nothing is true. The nihilistic and chaotic implications of disinformation are very much part of the design.

Even as the bulk of Russian disinformation targeted Trump supporters, operatives also went after Clinton and Sanders supporters, often with the apparent goal of radicalizing them, stirring emotions and anger. Again, arguably the most impactful Russian operation in 2016 had nothing to do with disinformation, but rather was the massive dump of hacked DNC emails through WikiLeaks. By releasing stolen emails, Russia aimed to—and arguably succeeded in—perpetuating negative stories about Hillary Clinton and sowing derision and internecine conflict within the Democratic Party. Chaos, not just supporting Trump, was the intent.

If we take the goal to be disorder, then the disinformation efforts of the past three years in the United States have been an enormous and unqualified success. Even if there is no definitive evidence disinformation campaigns (on their own) swung the 2016 election, they did manage to convince many people that they had done exactly that. It seems plausible that Russian social media meddling was just as much intended to spread distrust and conflict in Washington as anything else. While most Americans still get their news from reputable sources, many voters have grown far more skeptical of much of what they read—and whether their fellow citizens can be trusted. Even if false news stories on Twitter and Facebook are widely disbelieved, they can still drown out legitimate stories about politics and events.

Disinformation, in short, is about discrediting. From elections to the media to partisan politics to the institutions of Congress and the Presidency—doubt and chaos and distrust have very much conquered the United States. Only a concerted and sober effort to rebuild trust can win them back.

Several studies have cast doubt on the ability of disinformation to change ideological perspectives and political outcomes.
While each country’s legal framework, political environment, and social media landscape is unique, U.S. experience with online disinformation in the 2016 and 2018 elections offers several key lessons that can be useful for other countries, including in Latin America—in part due to the extensive empirical research on the nature and impact of online disinformation in these elections. It also offers an opportunity to consider the extent to which relevant stakeholders, particularly technology companies, applied lessons learned from the challenges that emerged in 2016 in the context of recent Latin American elections.

Following the best practices developed by Ann Ravel, Samuel Woolley, and Hamsini Sridharan, Latin American governments should think about the threat of disinformation through five distinct democratic principles: “transparency, accountability, standards, coordination, and adaptability.” These best practices, which are worth reading in full, emphasize thinking about democratic debate and discourse online in an inclusive and dynamic way, including establishing clear standards of transparency and accountability, as well as enabling coordination between government agencies, technology companies, and civil society actors.

The following recommendations aim to distill relevant lessons from the foregoing analysis of U.S. experience for relevant stakeholders in governments, technology companies, and civil society.

GOVERNMENTS

• **Social media matters.** In the weeks following the 2016 election, Facebook was the site most consulted for political information in the United States, with 21% of users, compared to just 2% for the Washington Post and 1.3% for the New York Times. Social media’s role as a digital “public square” is already formidable and likely only to grow. As such, the democratizing function of social media should be protected, even as governments and societies remain attentive to the impact of disinformation, the power and reach of which are dramatically amplified by social media.

• **Maintain perspective and avoid overreach.** While the empirical research regarding the impact of disinformation on voter behavior is not entirely conclusive, it suggests that even vast exposure to disinformation (one in four Americans visited a fake news website in 2016) may have only a minimal impact on the electoral process. Disinformation might have additional pernicious effects on democracy that warrant careful consideration, but evidence from the U.S. experience in 2016 argues in favor of a rigorous, careful approach to the challenge of disinformation that avoids overreach. Policy solutions that make governments the arbiter of the truth or authorize prior censorship are not only inconsistent with freedom of expression standards but unsupported by the existing evidence.

• **Focus on social media advertising.** The financial incentive of advertising revenue may be connected to the proliferation of disinformation. Platforms can sharply curtail both, either voluntarily or if necessary, through regulation. At a minimum, full transparency should be required regarding the identity and geographic location of any entity purchasing political advertising online.

• **Follow disinformation where it goes.** Disinformation will naturally track users to the platforms and online spaces they utilize most. In the United States, Russian operatives quickly found Instagram to be most effective and shifted many of their resources there. In Latin America, messaging platforms like WhatsApp are likely to play an outsized role, as was the case in Brazil. The characteristics of particular platforms—such as the peer-to-peer, encrypted nature of WhatsApp—will demand tailored solutions.

• **Be agile.** One of the biggest challenges in responding to online disinformation is that governments are often several steps behind from the beginning. Governments must develop monitoring and enforcement strategies that are proactive, and not reactive. This includes the ability to quickly expose disinformation and foreign intervention. While the U.S. intelligence community had been tracking Russia’s Internet Research Agency for years, there was no serious effort to identify and publicize their activities until after the 2016 election.

• **Improve information security and data protection.** While the political impact of disinformation is debatable, the consequences of hacking and information theft are far clearer. Politicians, governments, political parties, and other public sector organizations must modernize and strengthen their information security infrastructure or risk escalating attacks. Protecting citizens’ data privacy, including by strengthening legislation where necessary, is also critical.
TECHNOLOGY COMPANIES

- **Take (a share of) responsibility.** Following the 2016 U.S. elections, Facebook CEO Mark Zuckerberg famously dismissed the idea that propaganda and disinformation on his company's platform influenced the outcome, a statement he later said he regretted. Social media companies have always jealously guarded their status as mere conduits of content, wary of crossing the line from platform to publisher lest they be held liable for the content they host. In practice, however, they remain very far from this line, and as Zuckerberg subsequently acknowledged, the experience of 2016 showed that the evolution of the major social media platforms as democratic protagonists means they must play an active role in the search for solutions to online disinformation and related challenges.

- **Adapt the algorithms.** Algorithms that determine what information users see can be evolved to incorporate measures of information quality, rather than simply the information most likely to keep users glued to a site—especially where such information has been identified as disinformation or artificially promoted by bots. Social media platforms should, to the extent reasonable, make algorithmic information available to the public so that users understand why they are seeing the content they see. Content oversight bodies established by companies should have full access to algorithmic data necessary to their oversight function.

- **Maximize transparency.** Information about who purchases political advertisements online should be readily visible to users, as should the country from which page administrators most commonly access their accounts (with administrators prevented from using virtual private networks to disguise their locations).

CIVIL SOCIETY

- **Promote digital literacy.** Research suggests that voters are savvier and less susceptible to disinformation than is sometimes assumed. In the 2016 elections, voters over 60 were most susceptible to disinformation, suggesting that digital literacy plays a role in citizens' capacity to detect and discount disinformation. In the long-term, healthy democracies will need to be inoculated against the falsehoods enabled by the digital age, especially as purveyors of disinformation grow more sophisticated (to include synthetic media or so-called deepfake videos).

- **Expand research.** Social scientists have dedicated significant resources to understanding online disinformation in the 2016 U.S. elections, helping shed light on the extent and impact of this phenomenon. As disinformation itself evolves, so too will the need for continuing research to ensure that policy solutions are grounded in empirical reality. Platforms should provide researchers access to the necessary information while scrupulously protecting user data.

- **Iterate on fact-checking.** Fact-checking is a logical and laudable response to the challenge of disinformation. Evidence from the 2016 U.S. elections, however, suggests that fact-check and disinformation sites are disjointed and rarely reach the same users. This is not a reason to give up, but rather to continue experimenting with fact-checking solutions and measuring their impact.

- **Remember the big picture.** Disinformation's power is in amplifying and exploiting divisions, distrust, and norm violations in the real-world political sphere. Cleaning up online spaces is only half of the puzzle when it comes to improving democratic discourse. From politicians and political parties to multinational corporations and media outlets, the task of restoring citizens' faith in institutions and restoring facts and civility to the public sphere goes well beyond the specific challenge of online disinformation.
ENDNOTES

1 Ben Raderstorf is a non-resident fellow at the Inter-American Dialogue and a Master's in Public Policy candidate at the University of California, Berkeley. Michael Camilleri is Director of the Peter D. Bell Rule of Law Program at the Inter-American Dialogue.


5 Ibid.

6 Ibid.

7 Ibid.

8 Ibid.


Ibid.


Lubbers, Eric. 2016. “There is no such thing as the Denver Guardian, despite that Facebook post you saw.” The Denver Post. Online: https://www.denverpost.com/2016/11/05/there-is-no-such-thing-as-the-denver-guardian/


Ibid.

Ibid.

Kessler, Glenn, Salvador Rizzo, and Meg Kelly. 2019. “President Trump made 8,158 false or misleading claims in
his first two years.” The Washington Post. Online: https://www.washingtonpost.com/politics/2019/01/21/president-trump-made-false-or-misleading-claims-his-first-two-years/?noredirect=on&utm_term=.0ee3545bc0c7


48 Ibid.

49 Ingram, Matthew. 2018. “Most Americans say they have lost trust in the media.” Colombia Journalism Review. Online: https://www.cjr.org/the_media_today/trust-in-media-down.php


51 Ibid.


53 See Gov Track. 2019. “H.R. 2592 — 116th Congress: To enhance transparency and accountability for online political advertisements by requiring those who purchase and publish such ads to disclose information about the advertisements to the public, and for other purposes.” Online: https://www.govtrack.us/congress/bills/116/hr2592.


57 Ibid., pp 5.


61 Ibid.

Implications for Latin America


67 Ibid.


70 Spenkuch, Jörg and David Toniatti. 2018. “Political Advertising and Election Results.” Online: https://www.kellogg.northwestern.edu/faculty/spenkuch/research/advertising.pdf


81 Ibid.

About the Peter D. Bell Rule of Law Program

Established in 2015 with support from the Ford Foundation and named in honor of a founding Dialogue co-chair, the Peter D. Bell Rule of Law Program aims to elevate policy discussions around corruption and transparency, democracy and human rights, and citizen security in the Americas.

About the Inter-American Dialogue

The Inter-American Dialogue engages our network of global leaders to foster democratic governance, prosperity, and social equity in Latin America and the Caribbean. Together, we work to shape policy debate, devise solutions, and enhance cooperation within the Western Hemisphere.

www.thedialogue.org

Inter-American Dialogue
1155 15th St. NW, Suite 800 Washington, DC 20005
Tel: 202-822-9002