Fighting Digital Disinformation

Since the 2016 election, investigations, congressional hearings, academic research, and countless news stories have detailed the efforts by foreign actors to influence our elections by spreading false information on social media platforms. But four years later, our country is hardly better prepared to protect itself.

Disinformation was one of several potent strategies that the Russian government employed to influence the 2016 election. In the aftermath of the the election, experts studied thousands of posts from major social media platforms and found that the Russian Internet Research Agency (IRA) sought to benefit the Republican party by creating fraudulent accounts on social media sites like Twitter and Facebook and using them to post and spread false and inflammatory information. These efforts had three main goals: creating deeper divisions among voters on particular issues; discrediting or promoting particular candidates; and suppressing the vote.

One expert estimated that during the 2016 election, there was a "one-to-one ratio of junk news to professional news" shared on Twitter. Despite Mark Zuckerberg's insistence that it was "crazy" to think that false news had influenced the 2016 election's outcome, the company later admitted that "malicious actors" had engaged in disinformation campaigns on the site leading up to the 2016 election, including using inauthentic accounts to promote false news stories and direct people toward stolen data. Although there has never been a full accounting of the IRA's efforts, one report estimates that between 2015 and 2017, over 30 million Facebook and Instagram users shared the IRA's content.

These disinformation efforts did not target all Americans equally: they sought to polarize and disenfranchise particular groups -- chiefly Black voters. According to one report, Black voters were targeted in an effort to get them to boycott the election and focus on other methods of political engagement. Conservatives, Muslim Americans, LGBTQ+ and younger people were targeted as well, but the number of ads purchased on Facebook related to Black politics and culture or Black identity and nationalism far outstripped other audience segments.

As the 2020 election approaches, Russian disinformation is not the only threat we face online. The same tactics employed by the Russian government are just as easily accessible to domestic groups seeking to promote or oppose candidates and political or social issues.

Tech companies are trying to assure the public they have changed. But their efforts are no more than nibbles around the edges: periodic purges of inauthentic accounts, banning political ads on some platforms, and slow, inconsistent fact-checking. The same fundamental threats to our elections remain.

Disinformation erodes our democracy, and Democrats must have a plan to address it. Donald Trump has welcomed foreign interference in our elections, inviting interference from a host of countries that have an interest in the outcome, including Iran and China. He's currently facing impeachment for putting his own political interests over the national interests of the United States - and there is every indication that if he is not removed from office, he will continue to do so.

Anyone who seeks to challenge and defeat Donald Trump in the 2020 election must be fully prepared to take on the full array of disinformation that foreign actors and people in and around the Trump campaign will use to divide Democrats, suppress Democratic votes, and erode the standing of the Democratic nominee. And anyone who seeks to be the Democratic nominee must condemn the use of disinformation and pledge not to knowingly use it to benefit their own candidacy or damage others.

My Promise to Fight Disinformation as a Candidate

To truly stem the spread of damaging false information, tech companies and the federal government need to take a more serious, comprehensive approach. But I'm committed to doing everything I can do to combat disinformation, and that means tackling it on the campaign trail.

It's not enough to make vague statements condemning fraudulent attacks on opponents or efforts to suppress the vote -- while also reaping the benefits of those attacks on democracy. Campaigns need to make clear that disinformation has no place in our campaigns, and that we will disavow supporters who embrace it and act quickly to stop its spread. **That's why I'm pledging to fight disinformation aimed at my campaign, my opponents, and voters:**

- My campaign will not knowingly use or spread false or manipulated information, including false or manipulated news reports or doctored images, audio, and videos on social media.

- My campaign will not knowingly promote content from fraudulent online accounts.

- My campaign will not knowingly allow campaign staff or surrogates to spread false or manipulated information on social media.

I'm sending a clear message to anyone associated with the Warren campaign: I will not tolerate the use of false information or false accounts to attack my opponents, promote my campaign, or undermine our elections. And I urge my fellow candidates to do the same.

Holding Tech Companies Responsible for the Spread of Disinformation

Tech companies like Facebook, Twitter, and Google -- as well as other platforms like TikTok and Reddit -- have become essential to the ways Americans communicate and share information with each other. But the drive to maximize profit shapes how these companies design their platforms, prioritize the information users see, and police the use of their platforms. And often, that quest for profit contributes to the spread of disinformation.

For example, Facebook changed its policies to allow users to instantaneously share information to groups, a troubling way to quickly spread disinformation to millions of users. Google-owned YouTube has had to make changes to its algorithm to prevent it from feeding viewers misinformation. Both Twitter and Facebook have purged fake accounts in response to intense public scrutiny, but the negative response from investors leaves doubt as to whether these companies will commit to policing fake accounts in the long term. And I have already called out Facebook for permitting political candidates to run plainly false ads on its platform.

The safety of our democracy is more important than shareholder dividends and CEO salaries, and we need tech companies to behave accordingly. **That's why I'm calling on them to take real steps right now to fight disinformation.** I'm calling on Mark Zuckerberg of Facebook and Instagram, Jack Dorsey of Twitter, Susan Wojcicki of YouTube, and the CEOs of all large social media platforms to:

- *Work with other platforms and government to share information and resources:* A coordinated push to address disinformation will be far more effective than isolated efforts. When companies share information -- to the extent allowed under privacy laws -- they can better identify cross-platform disinformation campaigns and alert law enforcement officials of threats. This coordination will help identify and remove fraudulent accounts, deter the spread of disinformation, and rein in illegal activity.

- *Clearly label content created or promoted by state-controlled organizations*: When the organizations spreading information online are funded by foreign governments, it adds important context to the information they share. When Russia-run media organization Russia Today changed its name to RT, it obscured the fact that it is a state-controlled news outlet. Facebook announced last year that it would start labeling content created by state-controlled organizations, but it has not yet followed through on that promise. YouTube has inconsistently implemented its policy to label state-controlled media, allowing more than 50 channels to play content without a disclaimer. Social media companies should move swiftly to label all types of content created or promoted by state-controlled organizations -- and they should be clear about their policies for doing so.

- *Take meaningful steps to alert users affected by disinformation campaigns*: Even when social media companies like Facebook identify efforts at promoting disinformation, the steps they take to stem its corrosive effects are meager at best. Twitter notified users who had interacted with tweets from the IRA, and Facebook created a tool in its Help Center that allows users to see whether they liked or followed a page associated with the IRA. But social media companies can go much further: they should alert individuals who have interacted with fraudulent accounts regardless of their origin, and they should prevent sharing of content that was disseminated by fraudulent accounts.

- *Create clear consequences for accounts that attempt to interfere with voting:* One of the most harmful forms of political disinformation on social media is false information aimed at keeping people from exercising their right to vote. Facebook and Twitter have focused their efforts on banning fake accounts and identifying foreign interference, but not all disinformation comes from fake accounts or foreign interests. Social media platforms should ban accounts that knowingly disseminate false information about the time, place, and manner of voting.

- *Open up data for research*: Research by academics and watchdog organizations has provided the public with important insights into how disinformation spreads online, but these efforts are greatly limited by social media platforms' unwillingness to share data. Platforms like Facebook currently provide only limited and inconsistent access. Research can help evaluate the extent of, and patterns within, disinformation on social media platforms. It can also offer the public an objective evaluation of how the features that platforms offer, including those that allow for rapid dissemination of content, contribute to disinformation. Social media companies must provide an open and consistent application programming interface (API) to researchers.

- *Share information about algorithms and allow users to opt out of algorithmic amplification.* Algorithms decide what information users see and don't see on social media platforms -- and experts worry that they work to promote false or misleading information. Social media platforms owe the public insight into how these algorithms that affect their lives so deeply actually function. Increased transparency would allow researchers and policymakers to understand how algorithms contribute to the spread of disinformation, and it would give the public more insight into how their worlds are shaped by companies' decisions about what information they will or will not see. Further, users should have more choice in determining how their data and preferences are used to influence the information they see. Social media platforms should allow users to understand how algorithms affect their use of the platform, and to opt out of algorithmic amplification.

Companies like Facebook, Twitter, and Youtube can take these actions right now to stem the spread of disinformation. They should.

Government Actions to Address Disinformation

In addition to the steps that campaigns and the tech companies can take by themselves, I will take a series of actions as President to further address the spread of disinformation:

- *Push to create civil and criminal penalties for knowingly disseminating false information about when and how to vote in U.S. elections*: Voter suppression efforts of any kind offend basic American values. In both the 2016 and 2018 elections, online disinformation sought to depress voter turnout by telling people they could vote via text, giving people the wrong date for election day, and more. I will push for new laws that impose tough civil and criminal penalties for knowingly disseminating this kind of information, which has the explicit purpose of undermining the basic right to vote.

- *Reinstate the position of cybersecurity coordinator at the National Security Council*: The Trump Administration eliminated this critical position, weakening our defenses against cybersecurity threats and disinformation. As President, I will reinstate the position and empower the coordinator so that our country is safe.

- *Convene a summit of countries to enhance information sharing and coordinate policy responses to disinformation*: Countries around the world are struggling to address disinformation -- and certain governmental and non-governmental actors are targeting multiple countries. As President, I will push to convene a summit of countries dedicated to addressing this problem so that they can share information and coordinate responses to disinformation.

- *Establish rules around information and data sharing to ensure that platforms can share with each other and with the government while respecting individuals' privacy*: Both the government and major tech companies have access to information that can be helpful in identifying sources of disinformation. My administration will encourage robust data sharing between tech companies and between those companies and the government so that disinformation can be quickly identified and addressed -- while at the same time crafting those rules so that both the government and tech companies respect individual privacy. I will also push to institute a standard for public disclosure when the government identifies accounts conducting foreign interference so that Americans who have interacted with those accounts are notified.

- *Consider additional sanctions against countries that engage in election interference through disinformation*: In the case of Russian interference, this would include sanctions for financial institutions that supported interference, Russia's cyber sector, and people in Valdimir Putin's orbit who supported and facilitated interference.

The stakes of this election are too high -- we need to fight the spread of false information that disempowers voters and undermines democracy. I'll do my part -- and I'm calling on my fellow candidates and big tech companies to do their part too.