PHYS.ORG

How tech firms have tried to stop disinformation and voter intimidation, and come up short

November 3 2020, by Scott Shackelford

Credit: Unsplash/CC0 Public Domain

Neither disinformation nor voter intimidation is anything new. But tools developed by leading tech companies including Twitter, Facebook and

Google now allow these tactics to scale up dramatically.

As a scholar of cybersecurity and election security, I have argued that these firms must do more to rein in disinformation, digital repression and voter suppression on their platforms, including by treating these issues as a matter of corporate social responsibility.

Earlier this fall, Twitter announced new measures to tackle disinformation, including false claims about the risks of voting by mail. Facebook has likewise vowed to crack down on disinformation and voter intimidation on its platform, including by removing posts that encourage people to monitor polling places.

Google has dropped the Proud Boys domain that Iran allegedly used to send messages to some 25,000 registered Democrats that threatened them if they did not change parties and vote for Trump.

But such self-regulation, while helpful, can go only so far. The time has come for the U.S. to learn from the experiences of other nations and hold tech firms accountable for ensuring that their platforms are not misused to undermine the country's democratic foundations.

Voter intimidation

On Oct. 20, registered Democrats in Florida, a crucial swing state, and Alaska began receiving emails purportedly from the far-right group Proud Boys. The messages were filled with threats up to and including violent reprisals if the receiver did not vote for President Trump and change their party affiliation to Republican.

Less than 24 hours later, on Oct. 21, U.S. Director of National Intelligence John Ratcliffe and FBI Director Christopher Wray gave a briefing in which they publicly attributed this attempt at voter intimidation to Iran. This verdict was later corroborated by Google, which has also claimed that more than 90% of these messages were blocked by spam filters.

The rapid timing of the attribution was reportedly the result of the foreign nature of the threat and the fact that it was coming so close to Election Day. But it is important to note that this is just the latest example of such voter intimidation. Other recent incidents include a robo-call scheme targeting largely African American cities such as Detroit and Cleveland.

It remains unclear how many of these messages actually reached voters and how in turn these threats changed voter behavior. There is some evidence that such tactics can backfire and lead to higher turnout rates in the targeted population.

Disinformation on social media

Effective disinformation campaigns typically have three components:

A state-sponsored news outlet to originate the fabricationAlternative media sources willing to spread the disinformation without adequately checking the underlying factsWitting or unwitting "agents of influence": that is, people to advance the story in other outlets

The advent of cyberspace has put the disinformation process into overdrive, both speeding the viral spread of stories across national boundaries and platforms with ease and causing a proliferation in the types of traditional and social media willing to run with fake stories.

To date, the major social media firms have taken a largely piecemeal and fractured approach to managing this complex issue. Twitter announced a ban on political ads during the 2020 U.S. election season, in part over concerns about enabling the spread of misinformation. Facebook opted for a more limited ban on new political ads one week before the election.

The U.S. has no equivalent of the French law barring any influencing speech on the day before an election.

Effects and constraints

The impacts of these efforts have been muted, in part due to the prevalence of social bots that spread low-credibility information virally across these platforms. No comprehensive data exists on the total amount of disinformation or how it is affecting users.

Some recent studies do shed light, though. For example, one 2019 study found that a very small number of Twitter users accounted for the vast majority of exposure to disinformation.

Tech platforms are constrained from doing more by several forces. These include fear of perceived political bias and a strong belief among many, including Mark Zuckerberg, in a robust interpretation of free speech. A related concern of the platform companies is that the more they're perceived as media gatekeepers, the more likely they will be to face new regulation.

The platform companies are also limited by the technologies and procedures they use to combat disinformation and voter intimidation. For example, Facebook staff reportedly had to manually intervene to limit the spread of a New York Post article about Hunter Biden's laptop computer that could be part of a disinformation campaign. This highlights how the platform companies are playing catch-up in countering disinformation and need to devote more resources to the effort.

Regulatory options

There is a growing bipartisan consensus that more must be done to rein in social media excesses and to better manage the dual issues of voter intimidation and disinformation. In recent weeks, we have already seen the U.S. Department of Justice open a new antitrust case against Google, which, although it is unrelated to disinformation, can be understood as part of a larger campaign to regulate these behemoths.

Another tool at the U.S. government's disposal is revising, or even revoking, Section 230 of the 1990s-era Communications Decency Act. This law was designed to protect tech firms as they developed from liability for the content that users post to their sites. Many, including former Vice President Joe Biden, argue that it has outlived its usefulness.

Another option to consider is learning from the EU's approach. In 2018, the European Commission was successful in getting tech firms to adopt the "Code of Practice on Disinformation," which committed these companies to boost "transparency around political and issue-based advertising." However, these measures to fight disinformation, and the related EU's Rapid Alert System, have so far not been able to stem the tide of these threats.

Instead, there are growing calls to pass a host of reforms to ensure that the platforms publicize accurate information, protect sources of accurate information through enhanced cybersecurity requirements and monitor disinformation more effectively. Tech firms in particular could be doing more to make it easier to report disinformation, contact users who have interacted with such content with a warning and take down false information about voting, as Facebook and Twitter have begun to do.

Such steps are just a beginning. Everyone has a role in making democracy harder to hack, but the tech platforms that have done so much to contribute to this problem have an outsized duty to address it.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: How tech firms have tried to stop disinformation and voter intimidation, and come up short (2020, November 3) retrieved 11 July 2024 from https://phys.org/news/2020-11-tech-firms-disinformation-voter-intimidation.html