

# Online ads still vulnerable to manipulation in US election

31 January 2020, by Barbara Ortutay and Amanda Seitz



In this April 26, 2019, file photo, visitors to New York's Times Square use umbrellas to shield themselves against the rain as they walk past the Armed Forces Recruitment Center. Before Election Day, politicians are expected to spend more than \$1 billion to pelt voters with millions of cheap online ads, which can be tailored to a voter's most personal details—down to one household or even a single individual. (AP Photo/Mary Altaffer, File)

Older men in Arkansas might see a close-up photo of President Donald Trump pumping his fist in the air, along with a message asking them to donate \$30 to his campaign for a Super Bowl commercial.

Middle-aged women in California might see a photo of Trump pointing to a crowd, with a plea for them to give "any amount" to the campaign.

Before Election Day, politicians are expected to spend more than \$1 billion to pelt voters with millions of these cheap online ads, which can be tailored to a voter's most personal details—down to one household or even a single individual.

Experts warn that this ad-targeting system is still vulnerable to manipulation by [foreign governments](#)

and domestic grifters trying to influence the election, just as they did in 2016. Those attempts could become more sophisticated this year as tech companies wrestle with a dysfunctional federal election watchdog agency and deploy haphazard safeguards that still offer plenty of loopholes.

"There's now so much money and attention spent online with so few rules that if you wanted chaos, that's the place to go for chaos," said David Karpf, a political communications professor at The George Washington University. "And there's a bunch of people who want chaos."

Russia-connected accounts spent just \$100,000 on Facebook ads during the 2016 presidential election to fan division on polarizing issues such as gun control and race relations. That's a fraction of the cost of a single 30-second spot on a major TV network.

But it was enough to stir up trouble. In response, Google, Facebook and Twitter instituted verification policies that require advertisers to confirm their identity using their organization's tax identification number or other government ID. Twitter later banned all [political ads](#).

"Microtargeting" allowed the divisive messages to reach small pockets of voters in certain geographical locations based on their specific interests.

Google this month began limiting U.S. advertisers' ability to target political ads beyond broad categories such as sex, age and postal code. Facebook will continue to allow campaigns to target voters for any reason, down to their most personal interests.

Such targeting technology offers distinct advantages.

A candidate running a TV spot might reach a

specific audience watching the show "The Real Housewives of Atlanta." But on Facebook that same candidate can run a specific ad aimed at Atlanta housewives who lean moderate, like to hunt and hold a master's degree, for instance.

In Texas, for example, Republican strategist Chris Wilson said his polling found suburban women were frustrated by red-light cameras, so he targeted thousands of them on Facebook with ads promising that his client GOP Gov. Greg Abbott would abolish the cameras if elected to a second term in 2018.

Abbott won and signed a law last summer banning red-light cameras in the state. Wilson argues that microtargeting helps to mobilize voters around certain issues.

Google and Facebook have spent years collecting troves of data that now help campaigns persuade voters, said Luca Cian, a professor at the Darden School of Business who focuses on how marketing affects [political campaigns](#).

"I can specify that one person in one specific household should see a specific ad," he said. "And their neighbor could see a different ad."

It's not just campaigns running ads. With the click of a button and a few hundred dollars, ordinary people or businesses can now purchase political ads that are directed at specific groups of people to see.

The sheer volume of ads makes it nearly impossible to track them.

"How does anybody even begin to try and keep up and monitor tens of thousands ... or maybe millions of ads?" asked Ellen Weintraub, chairwoman of the Federal Elections Commission, the taxpayer-funded watchdog agency that creates and enforces rules for federal campaigns.

That's a problem for journalists seeking to hold politicians accountable and for opposing candidates who might unwittingly be featured in an attack ad by political rivals.

In nearly every type of race—from city council

candidates to the presidential election—campaigns might struggle to spot false claims running about their candidate online, said Democratic campaign consultant Jared Kamrass.

"If a negative ad is run against my candidate on digital, I almost have no way of knowing about it unless someone screenshots it," Kamrass said.

Since the last [presidential election](#), tech companies have considered many questions: Should they allow political ads at all? Fact-check them? Catalog them in a public database? Prevent them from being targeted to small groups of people?

Some companies adopted their own rules for political ads. Twitter, which made little money off the ads, took the most radical step. In November, CEO Jack Dorsey announced the site would reject all political ads from its platform worldwide.

The [tech companies](#) have been left to regulate themselves, in part, because the FEC has been gridlocked for years over rules that would be tailored to the booming online political ad industry. The agency is without a full set of leaders and does not have a quorum needed to consider new rules for ads or to penalize campaigns for violating the law.

"We end up in kind of the messy state we're in when your regulators stop regulating and there's a ton of money in the system," Karpf added. "Of course that's going to end up going haywire."

Facebook has stuck to its plan of prohibiting third-party fact checkers from rating political ads as false, despite widespread criticism from politicians such as Democratic presidential candidate Sen. Elizabeth Warren.

The social network has acknowledged that the tools aren't perfect. Sarah Schiff, a Facebook product manager, said the goal is to make it "more difficult" for bad actors to misuse the platform.

Even smaller platforms, including TikTok and Pinterest, have been forced to confront the issue by banning political ads entirely, as has the Microsoft-owned LinkedIn. But none of those rules is

foolproof.

Experts say political campaigns, foreign government and trolls will continue to push the boundaries, testing to see which messages, images or videos resonate with potential voters based on their data.

"For democracy to work, you need a common reality, which means a common understanding of who's saying what when," said Daniel G. Newman, the president of MapLight, a nonprofit that tracks political money, lobbying and votes. "But when politicians are saying different things to different audiences, even thousands of different small audiences, there's an inability to hold them accountable."

© 2020 The Associated Press. All rights reserved.

APA citation: Online ads still vulnerable to manipulation in US election (2020, January 31) retrieved 23 September 2020 from <https://techxplore.com/news/2020-01-online-ads-vulnerable-election.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*