TIME

Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You

A Facebook Like Button logo is seen at the entrance of the Facebook headquarters in Menlo Park, Calif., on May 10, 2012.
Kimihiro Hoshino—AFP/GettyImages

IDEAS

BY **DIPAYAN GHOSH AND BEN SCOTT** MARCH 19, 2018

Ghosh, a White House technology and economic adviser from 2014–2015 and former privacy policy expert at Facebook, is a Fellow at New America and the Shorenstein Center at the Harvard Kennedy School; Scott, a Policy Advisor for Information in the U.S. State Department from 2010–2012, is Senior Advisor at New America.

The questions surrounding the role of Facebook and other social media sites in the politics of our time have been coming at what feels like an accelerating pace. Reporting by the *Observer*, the *Guardian* and the New York

Times in recent days has revealed that Cambridge Analytica — the social media monitoring firm that bragged it helped put Trump in the White House — had gained access before the election to the data of 50 million Facebook users through highly questionable means. Cambridge Analytica used to that data to create a tool of "psychological warfare" to manipulate American voters with targeted Facebook ads and social media campaigns. This news has painted the national discussion over social media's impact on national politics in a stark new light. There was already a debate raging about how targeted digital ads and messages from campaigns, partisan propagandists and even Russian agents were sowing outrage and division in the U.S. electorate. Now it appears that Cambridge Analytica took it one step farther, using highly sensitive personal data taken from Facebook users without their knowledge to manipulate them into supporting Donald Trump. This scandal raises major questions about how this could have happened, how it can be stopped and whether the connection between data-driven ads and democracy is fundamentally toxic.

The bombshells are dropping so fast in this story about social media and the 2016 election, it is hard to keep up. Recall that just last week, Washington was aflutter over allegations from Brad Parscale, head of digital media strategy for President Donald Trump's 2016 presidential run and the man who led the partnership with Cambridge Analytica, who tweeted on February 24 that his boss' campaign had a massive advantage using Facebook advertising to reach voters. Parscale, who is now chief of Trump's 2020 efforts, said his candidate's Facebook ads were 100 or 200 times more cost-effective than those placed by the Clinton campaign for the presidency. Facebook quickly shared proprietary data illustrating that the two campaigns paid roughly the same aggregate sums to reach voters — and that the Trump campaign actually paid more on average than the Clinton campaign.

Now in light of the Cambridge Analytica headlines, it is clear that *price* of the advertising wasn't the real story. The real story is about how personal data from social media is being used by companies to manipulate voters and distort democratic discourse. In this regard, it appears the Trump campaign had a decisive and ill-gotten advantage in the quest to exploit personal data to influence voters. And they used it to the hilt.

This is all very alarming. And as the days follow and the details are parsed about how this happened and who is to blame for malign social media advertising, we should not lose sight of a more basic question. As they stand, are the ways that social media sites use personal data to sell and publish political ads good for democracy in the first place?

On the internet, you don't know much about the political ads you're shown. You often don't know who is creating them, since the disclaimers are so small, if they exist at all. You also don't really know who else is seeing them. Sure, you can share a political ad — thus fulfilling the advertiser's hopes — and then at least some other people you know will have witnessed the same ad. But you don't really know if your neighbor has seen it, let alone someone else across the state or the country. In addition, digital advertising companies distribute ads based on how likely you are to interact with them. This most often means that they send you ads they think you are likeliest to engage with. They don't determine what the nature of that engaging content might be — but they know (just as all advertisers do) that content works well if it makes you very emotional. An ad like that doesn't make you contemplative or curious, it makes you elated, excited, sad or angry. It could make you so angry, in fact, that you'll share it and make others angry — which in turn gives the ad free publicity, effectively making the advertiser's purchase cheaper per viewer, since they pay for the initial outreach and not the shares. (This last bit is precisely what made Parscale proud.)

What this can lead to is communities and, eventually, a nation infuriated by things others don't know about. The information that makes us angriest becomes the information least likely to be questioned. We wind up stewing

over things that, by design, few others can correct, engage with or learn from. A Jeffersonian public square where lots of viewpoints go to mingle, debate and compromise, this is not.

The reason you don't know about all of these things is the same reason that we as citizens should be worried: the whole system operates in the darkness of proprietary data and algorithmic processes at internet companies. Unless they tell us how they use the data they collect about us and design their targeting algorithms, we can only guess.

It's important to distinguish what is new about this process. There are similarities here to the world of broadcast political ads — which itself is a cesspool. If a campaign produces a profoundly noxious ad, it might get some extra coverage in the news about how the ad was especially outrageous, meaning more people see it but at no additional cost. But producing and buying airtime for a TV ad is a lot more expensive and reaches a lot fewer people than if a political organization can make a toxic ad go viral on Facebook, Twitter or YouTube and reach millions of people. Plus, when that organization does this on TV, it is transparent to everyone what it's doing because the ad is on TV, and the organization is required by law to put its name on the ad and survive regulatory scrutiny. If a political organization does the same thing on a social media platform, it is, again, only visible to the people you targeted and those they share it with. And labels showing who bought the ad are often not all that they could be. (The companies say they are fixing this — and if they don't, then regulation probably will compel it.)

TV stations also don't have nearly as much detailed information about what makes their viewers react. But social media sites do. This gives political groups and campaigns incredible power — and is the secret sauce of the Internet advertising business, since it also proffers commercial advertisers the same ability. Here's how it works.

First, the campaign collects as many email addresses from as many places as possible from potential supporters. Sometimes they take the voter file itself (the public list of all registered voters) and use data-mining techniques to

match names and home addresses with email addresses. Next, the campaign uploads that massive list of email addresses into a social media service. Facebook, for example, can match the email addresses to individual users to create a "Custom Audience." This is where Cambridge Analytica had a huge advantage, since they had the private Facebook data themselves and did not need to rely on guesswork to match email addresses and Facebook pages to actual voters. This audience can then be sliced and diced into different demographic groups, right down to people's political and cultural preferences and biases. Here again, Cambridge Analytica may well have used their own private data stash to figure out ways to target specific voters with specific messages by studying their past behavior on Facebook. These filtered groups can then be tested to see which people respond well to which messages. From there, Facebook has another tool called "Lookalike Audiences" — as do other sites – that will find people that are similar to those designated in any given slice of the Custom Audience. Then the campaign buys ads that deliver the messages that Facebook data confirms people want to hear — turning up the outrage and sensation factor to get attention (ideally for free).

All of this does not add up to sites like Facebook and Twitter intentionally undermining Hillary Clinton. It is simply the nature of ad tech and social media: use personal data to divide up classes of the American population like barn animals, then feed us highly personalized messages designed to push our particular buttons so well that we share them and they go viral, thus keeping people on the site longer. Social media rewards provocation — again, without repercussion, since we usually only share content with our friends in a way that is largely invisible to the broader public. Morality and integrity count little in online advertising.

The real question here isn't which campaign got the advantage. The real question is whether this micro-targeted free-for-all should be allowed in the political sphere at all in the way it is currently designed —with very little transparency about who is pulling these strings and how they are doing it.

When Russian trolls used social media to manipulate the voting public — apparently even more cost-effectively than the Trump campaign — it triggered

a national scandal along with demands that the social media companies be held accountable for letting it happen. But when our own political parties do this to us, we often turn a blind eye. It's politics as usual. Perhaps it is time to reconsider how and when we should set appropriate restrictions on the use of social media for political communications, especially as another set of national elections is just around the corner.

Beyond basic commitments to assure the privacy and security of their personal data, voters have a right to know who is trying to send them political messages and how they are doing it. They should know who bought the ads, how much they spent and what particular demographic audiences were targeted. They should be able to look at all the ads run by the people trying to reach them. This should not be a database available somewhere on the Internet that normal users would never visit. It should be pushed forward as a part of the ad, so that it is easy to click and see the data right there. Beyond that, social media sites should take action against any political communicator that tries to break the rules. Facebook has responded to the Cambridge Analytica story to say that the technique used to extract data from 50 million users is no longer allowed. But no one is sure exactly what types of sensitive personal data are already out there or who possesses them — making it likely that efforts at voter exploitation will continue. For this reason, the companies should continue to develop better algorithmic detection systems to discover attempts to mislead prospective voters and act against them before or soon after they are disseminated.

But the American public must be wary, since the drive toward total transparency is unlikely to come from the politicians currently in power — or the tech companies themselves, even after they adopt some laudable measures. If there is anything we should learn from the Cambridge Analytica revelations, it is that unless things change, we can expect the spread of disinformation and the systemic manipulation of voters to happen all over again, not only in U.S. national elections but throughout the world. Because if there's one thing everyone can agree on, it's that these tools are effective.

MOST POPULAR ON TIME

1. How to Make a DIY Face Mask for Coronavirus
2. Why Sweden's Lax Coronavirus Approach Could Be Backfiring
3. A Paramedic's Diary of One Week With Coronavirus Patients

CONTACT US AT EDITORS@TIME.COM**.**

TIME Ideas hosts the world's leading voices, providing commentary on events in news, society, and culture. We welcome outside contributions. Opinions expressed do not necessarily reflect the views of TIME editors.

TIME