The New York Times

OP-ED CONTRIBUTOR

Beware of A.I. in Social Media Advertising

By Dipayan Ghosh

March 26, 2018

Nine days ago, we learned that Cambridge Analytica, the firm engaged by the Trump campaign to lead its digital strategy leading up to the 2016 United States presidential elections, illegitimately gained access to the Facebook data of more than 50 million users, many of them American voters. This revelation came on the heels of the announcement made last month by the Justice Department special counsel Robert Mueller of the indictment of 13 Russians who worked for the Internet Research Agency, a "troll farm" tied to the Kremlin, charging that they wielded fake social media accounts to influence the 2016 presidential elections.

But as Facebook, Google, Twitter and like companies now contritely cover their tracks and comply with the government's requests, they simultaneously remain quiet about a critical trend that promises to subvert the nation's political integrity yet again if left unaddressed: the systemic integration of artificial intelligence into the same digital marketing technologies that were exploited by both Cambridge Analytica and the Internet Research Agency.

According to the F.B.I.'s findings, the tactics used to date by Russia have, technologically speaking, not been particularly sophisticated. Those tactics have included the direct control of fake social media accounts and manual drafting of subversive messages. These were often timed for release with politically charged incidents in the real world — including, for instance, the suicide bombings in Brussels, the declaration of Donald Trump as the Republican nominee and Mr. Trump's staging of a town hall in New Hampshire, each of which occurred weeks before election night in 2016. Further, according to various experts, Cambridge Analytica's targeting efforts likely were tame and ineffective.

Each step of the digital campaigns seems to have been orchestrated by a human working from a computer terminal. To be sure, we know that the Internet Research Agency's deception campaigns altogether enjoyed broad reach and were viewed by many Americans; more than 126 million of us may have unwittingly viewed the Russians' egregious and misleading content on Facebook alone. And if Cambridge Analytica did indeed make use of the rich trove of sensitive data it acquired from Aleksandr Kogan's firm Global Science Research, Cambridge Analytica's

content too likely reached tens of millions of American voters. But because their digital messaging was largely controlled directly by a bottleneck of human propagators, its spread necessarily was relatively uncoordinated and ad hoc.

As the industry increasingly integrates artificial intelligence into digital advertising, however, disinformation operations and legitimate political communications will gradually become concerted, automatic and seamless. The real innovation in digital marketing — and the type of thing that the United States Congress and American voters should be particularly concerned about — is the execution of disinformation that operates at real scale. Where there were once a couple dozen human operators stitching together a few divisive messages during working hours in Moscow to pick at the digital halls of our democracy, there will soon be countless A.I. systems testing and probing a plethora of content on a vast field of social media user audiences that are highly segmented by race, ethnicity, gender, location, socioeconomic class and political leaning. We can expect advisory firms like Cambridge Analytica, the Russians and other participants — not to mention our own political parties themselves — to pounce on this new vector for political messaging and take direct aim at our open political discourse.

Despite these myriad risks, industry professionals seem to have turned a blind eye to the oncoming specter of A.I., likely because they are optimistic about its commercial potential. The leading internet firms are offering free A.I. courses for their brightest engineers; are developing plans to integrate A.I. across their leading brands and products; and are staffing up with brilliant philosophers, ethicists and technocrats to deflect nosy regulators and win over the merchants of information. In his interview with The New York Times last week, Mark Zuckerberg even went so far as to describe A.I. as the antidote that will cure the internet of such negative externalities as hate speech and election interference. What internet firms are not transparent about, though, is the degree to which they plan to integrate A.I. into their principal profit-generating engine: digital advertising.

Consider the scale and complexity of the advertising ecosystem. Global internet firms like Facebook, Twitter, Snapchat and Google collectively enjoy billions of active users who on average spend more than two hours on these platforms every day. Each user might be shown hundreds or thousands of digital display ads — or "sponsored" content — within that time. People in the industry leverage an intricate web of ad agencies, exchanges, networks, demand-side platforms and supply-side platforms to manage the delivery of those ads around the clock.

But if you could remove those people from the equation, you could quietly turn a $100 billion digital ad industry into a $1 trillion persuasion machine.

To be clear, algorithms have long been part and parcel of the industry. Organizations like the Russian government and Cambridge Analytica were taking advantage of them simply by virtue of using social media for political communications. But the sharp uptick in industry research and development in A.I. over the past year strongly suggests that this new technology will soon be brought to bear in digital advertising. This will increase the speed of ad mediation, inundating

users with content finely tuned to their personal desires. It will abet the seamless and accurate development of “look alike” audiences, enabling advertisers to upload their customer lists and automatically send ads to like-minded people that they do not already know. And it will enable automated contingency-based marketing, allowing clients to programmatically trigger certain kinds of content to be shared in the moments after real world events transpire.

For students of disinformation — including the Russians who to date have not even had to leverage such sophisticated web technology to mislead American voters — this new information ecosystem presents a vast land of opportunity. One could imagine that the Internet Research Agency could set up automated, machine learning-informed content-targeting systems so that minutes after North Korea’s leader references a hypothetical ICBM, the Russians send inflammatory A.I.-produced messages and imagery to classes of the American population that A.I. has predicted will be susceptible to disinformation. The scalability of such activity is what makes such tactics especially fearsome.

Deep-rooted societal tensions will likely be exacerbated by the irresponsible integration of A.I. into digital advertising services — not to mention, into the ranking and curation of “organic” content on social media news feeds and search results. We’re already seeing this. For example, just a few hours before Senator Marco Rubio took the stage to speak with students from Marjory Stoneman Douglas High School, ill-taught algorithms were responsible for the spread of YouTube videos that mocked and shamed the students.

Even in light of the Cambridge Analytica revelations, there is time yet to act. Internet firms should aggressively work to limit disinformation on their platforms by developing algorithms — perhaps driven by A.I., as suggested by Mr. Zuckerberg — that can detect disinformation and flag it for fast human review. Strong one-off actions against widespread disinformation tactics, such as Twitter’s recent move, can also help. They also must be more transparent about their algorithmic software and data practices with researchers, journalists and consumers. Further, the regulatory community must continue its aggressive review of the industry’s practices. The Federal Trade Commission’s announcement of its forthcoming investigation into Facebook’s privacy practices represents excellent progress.

In the meantime, the public must not let up. The economic structure of the digital sector has already harmed our society in ways that have been exacerbated by the unchecked collection of individual behavioral data. The revelations about Cambridge Analytica and Russia’s disinformation operations are prime evidence for this — and things could get worse very soon. Politicians and regulators must continue the call for a meaningful privacy law and stronger antitrust enforcement in this country. Nothing less can win us back full control of the state.

Dipayan Ghosh is a fellow at New America and the Shorenstein Center at the Harvard Kennedy School. He has previously served as a technology and economic adviser to the Obama White House and as a United States privacy and public policy adviser at Facebook.

Follow The New York Times Opinion section on Facebook and Twitter (@NYTopinion), and sign up for the Opinion Today newsletter.