MIND GAMES
HOW CAMPAIGNS ARE USING MARKETING, MANIPULATION, AND ‘PSYCHOGRAPHIC TARGETING’ TO WIN ELECTIONS—AND WEAKEN DEMOCRACY

BY SUE HALPERN

ILLUSTRATIONS BY MATT CHASE
when the Senate Judiciary and Commerce committees summoned Facebook CEO Mark Zuckerberg to Washington, it looked as if the nation was finally going to reckon with the outsized role that technology companies now play in American elections. Seventeen months had gone by since Donald Trump’s stunning presidential victory—a success credited by many to his campaign’s mastery of Facebook’s advertising platform, as well as to the divisive agitprop seeded throughout Facebook by Russian trolls from the Internet Research Agency, whose 470 pages and accounts were seen by an estimated 157 million Americans.

But that was not what brought Zuckerberg to the Capitol. Instead, he was there to diffuse the bomb dropped three weeks earlier by Christopher Wylie, former research director at Cambridge Analytica, the data science firm that Trump’s digital team had employed during the election campaign. In interviews with The Guardian and The New York Times, Wylie confirmed that his company had taken data from millions of Facebook users without their knowledge or consent—as many as 87 million users, he later revealed. Cambridge Analytica had used the information to identify Americans’ subconscious biases and craft political messages designed to trigger their anxieties and thereby influence their political decisions—recasting a marketing technique known as “psychographics” that, more typically, is used to entice retail customers with ads that spark their underlying emotional reflexes. (“This product will make you feel happy!” “This product will make you feel attractive!”)

Cambridge Analytica turned this technique sideways, with messaging that exploited people’s vulnerabilities and psychological proclivities. Those with authoritarian sympathies might have received messages about gun rights or Trump’s desire to build a border wall. The overly anxious and insecure might have been pitched Facebook ads and emails talking about Hillary Clinton’s support for sanctuary cities and how they harbor undocumented and violent immigrants.

Alexander Nix, who served as CEO of Cambridge Analytica until March, had earlier called this method of psychological arousal the data firm’s “secret sauce.”

Cambridge Analytica had purchased its Facebook user data for more than $800,000 from Global Science Research (GSR), a company that was set up specifically to access the accounts of anyone who clicked on GSR’s “This Is Your Digital Life” app—and the accounts of their Facebook friends. At the time, Facebook’s privacy policy allowed this, even though most users never consented to handing over their data or knew that it had been harvested and sold. The next year, when it became aware that Cambridge Analytica had purchased the data, Facebook took down the GSR app and asked both GSR and Cambridge Analytica to delete the data. “They told us they did this,” Zuckerberg told Congress. “In retrospect, it was clearly a mistake to believe them.” In March, around the time Wylie came forward, The New York Times reported that at least some of the data was still available online.

Wylie, a pink-haired, vegan, gay Canadian, might seem an unlikely asset to Trump’s campaign. And as he tells the story now, he’s filled with remorse for creating what, in an interview with The Guardian, he referred to as “Steve Bannon’s psychological warfare mindfuck tool.” For months, he had been quietly feeding information to the investigative reporter Carole Cadwalladr, whose articles in The Guardian and The Observer steadily revealed a through-line from dark money to Cambridge Analytica to Trump. (Cadwalladr also connected Cambridge Analytica to the Brexit campaign, through a Canadian data firm that worked both for the Vote Leave campaign and for Cambridge Analytica itself.) When he finally went public, Wylie explained how, with financial support from right-wing billionaire Robert Mercer, Cambridge Analytica’s principal investor, and with Steve Bannon’s guidance, he had built the algorithms and models that would target the innate biases of American voters. (Ted Cruz was one of Cambridge Analytica’s first clients and was Mercer’s preferred presidential candidate in the primaries before Trump crushed him.) In so doing, Wylie told Cadwalladr, “We ‘broke’ Facebook.”

So Zuckerberg agreed to come to Washington to be questioned by senators about the way his company’s lax privacy policies had inadvertently influenced the U.S. election—and possibly thrown it to Donald Trump. But what should have been a grilling turned out to be more like a sous vide—slow, gentle, low temperature—as the senators lightly rapped Zuckerberg on his knuckles over Facebook’s various blunders, and he continually reminded them that he’d created the site in his Harvard dorm room, not much more than a decade before, and now look at it! Of course, he reminded them with a kind of earnest contrition, there were going to be bumps in the road, growing pains, glitches. The senators seemed satisfied with his shambling responses and his constant
refrain of “My team will get back to you,” and only mildly bothered when he couldn’t answer basic questions like the one from Roger Wicker, a Mississippi Republican, who wanted to know if Facebook could track a user’s internet browsing activity, even when that person was not logged on to the platform. (Answer: It can and it does.)

Shortly before this tepid inquest, Zuckerberg publicly endorsed the Honest Ads Act, a bipartisan bill cosponsored by Democratic Senators Amy Klobuchar and Mark Warner and Republican John McCain, which, among other things, would require internet platforms like Facebook to identify the sources of political advertisements. It also would subject online platforms and digital communications to the same campaign disclosure rules as television and radio.

A tech executive supporting federal regulation of the internet may, at first, seem like a big deal. “I’m not the type of person that thinks all regulation is bad,” Zuckerberg told the senators. “I think the internet is becoming increasingly important in people’s lives, and I think we need to have a full conversation about what is the right regulation, not whether it should be or shouldn’t be.” But Facebook has spent more than $50 million since 2009 lobbying Congress, in part to keep regulators at a distance, and cynics viewed Zuckerberg’s support for the new law as a calculated move to further this agenda. (Indeed, after California passed the strongest data privacy law in the country in June, Facebook and the other major tech companies began lobbying the Trump administration for a national, and far less stringent, data privacy policy that would supersede California’s.) Verbally supporting the Honest Ads Act—legislation that is unlikely to be enacted in the current atmosphere of the Congress—was easy, especially when Facebook had already begun rolling out a suite of new political ad policies that appeared to mirror the minimal transparency requirements lawmakers sought to establish. The subtext of this move was clear: Facebook could regulate itself without the interference of government overseers.

Zuckerberg’s congressional testimony was the culmination of an extensive apology tour in which he gave penitent interviews to The New York Times, Wired, Vox, and more, acknowledging that mistakes had been made. “This was a major breach of trust,” Zuckerberg told CNN. “I’m really sorry that this happened.” A month later, Facebook launched a major ad campaign, vowing, “From now on, Facebook will do more to keep you safe and protect your privacy.” Then, in mid-May, Cambridge Analytica declared bankruptcy, though this did not put an end to the whole affair. A legal challenge to the company by American professor David Carroll for processing his voter data without his knowledge or consent has been allowed to continue in the U.K., despite the firm’s dissolution.

It’s impossible to know whether Cambridge Analytica’s psychographic algorithms truly made a difference in Trump’s victory. But the underlying idea—that political campaigns can identify and influence potential voters more effectively by gathering as much information as possible on their identities, beliefs, and habits—continues to drive both Republican and Democratic data firms, which are currently hard at work on the next generation of digital campaign tools. And while the controversy surrounding Cambridge Analytica exposed some of the more ominous aspects of election campaigning in the age of big data, the revelations haven’t led to soul-searching on the part of tech companies or serious calls for reform by the public—and certainly not from politicians, who benefit most from these tactics.

If anything, the digital arms race is accelerating, spurred by advances in artificial intelligence and machine learning, as technologists working both sides of the political aisle develop ever-more-powerful tools to parse, analyze, and beguile the electorate. Lawmakers in Congress may have called Mark Zuckerberg to account for Facebook’s lax protection of its users’ data. But larger and more enduring questions remain about how personal data continues to be collected and used to game not just the system, but ourselves as sovereign individuals and citizens.

IN 1960, JOHN F. KENNEDY’S CAMPAIGN manager—his brother Robert—hired one of the first data analytics firms, the Simulmatics Corporation, to use focus groups and voter surveys to tease out the underlying biases of the public as the country considered whether to elect its first Catholic president.

The work was top secret; Kennedy denied that he’d ever commissioned the Simulmatics report. But in the decades that followed, as market researchers and advertisers
adopted psychological methods to better understand and appeal to consumers, social scientists consulting on political campaigns embraced the approach as well. They imagined a real-world political science fashioned out of population surveys, demographic analyses, psychological assessments, message testing, and algorithmic modeling. It would be a science that produced rational and quantifiable strategies to reach prospective voters and convert them into staunch supporters. That goal—merely aspirational at the time—has since developed into a multibillion-dollar industry, of which Cambridge Analytica was a well-remunerated beneficiary. For its five-month contract with the Trump campaign in 2016, the company was paid nearly $6 million.

The kind of work Cambridge Analytica was hired to perform is a derivative of “micro-targeting,” a marketing technique that was first adapted for politics in 2000 by Karl Rove, George W. Bush’s chief strategist. That year, and to an even greater degree in 2004, Rove and his team set about finding consumers—that is to say, voters—who were most likely to buy what his candidate was selling, by uncovering and then appealing to their most salient traits and concerns. Under Rove’s guidance, the Bush team surveyed large samples of individual voters to assess their beliefs and behaviors, looking at such things as church attendance, magazine subscriptions, and organization memberships, and then used the results to identify 30 different kinds of supporters, each with specific interests, lifestyles, ideologies, and affinities, from suburban moms who support the Second Amendment to veterans who love NASCAR. They then slotted the larger universe of possible Bush voters into those 30 categories and tailored their messages accordingly. This approach gave the Bush campaign a way to supplement traditional broadcast media by narrowcasting specific messages to specific constituencies, and it set the scene for every campaign, Republican and Democratic, that followed.

In 2008, the micro-targeting advantage shifted to the Democrats. Democratic National Committee Chair Howard Dean oversaw the development of a robust database of Democratic voters, while for-profit data companies were launched in support of liberal causes and Democratic candidates. Their for-profit status allowed them to share data sets between political clients and advocacy groups, something the DNC could not do with its voter database because of campaign finance laws. One of these companies, Catalist, now controls a data set of 240 million voting-age individuals, each an aggregate, the company says, of hundreds of data points, including “purchasing and investment profiles, donation behavior, occupational information, recreational interests, and engagement with civic and community groups.”

“Catalist was a game changer,” said Nicco Mele, the director of Harvard’s Shorenstein Center on Media, Politics, and Public Policy, and a veteran of dozens of political campaigns. “It preserved data in an ongoing way, cycle after cycle, so it wasn’t lost after every campaign and didn’t have to be re-created for the next one. Catalist got things going.”

The data sets were just one part of it. In 2008 and 2012, the Democrats also had more sophisticated predictive models than the Republicans did, a result of having teams of data scientists and behavioral scientists advising Barack Obama’s presidential campaigns. While the data scientists crunched the numbers, the behavioral scientists conducted experiments to determine the most promising ways to get people to vote for their candidate. Shaming them by comparing their voting record to their family members and neighbors turned out to be surprisingly effective, and person-to-person contact was dramatically more productive than robocalls; the two combined were even more potent.

The Obama campaign also repurposed an advertising strategy called “uplift” or “brand lift,” normally used to measure consumer-brand interactions, and used it to pursue persuadable voters. First they gathered millions of data points on the electorate from public sources, commercial information brokers, and their own surveys. Then they polled voters with great frequency and looked for patterns in the responses. The data points, overlaid on top of those patterns, allowed the Democrats to create models that predicted who was likely to vote for Obama, who was not, and who was open to persuasion. (The models also indicated who would be disinclined to vote for Obama if contacted by the campaign.) These models sorted individuals into categories, as the Bush campaign had done before—mothers concerned about gun violence, say, or millennials with significant college debt—and these categories were then used to tailor communications to the individuals in each group, which is the essence of micro-targeting.

The Obama campaign had another, novel source of data, too: information that flowed from the cable television
set-top boxes in people’s homes. Through agreements with industry research firms, the campaign sent them the names and addresses of individuals whom their models tagged as persuadable, and the research companies sent back anonymous viewing profiles of each one. The campaign used these profiles to identify which stations and programs would give them the most persuasion per dollar, allowing them to buy ads in the places and times that would be most effective. The campaign also mined—and here’s the irony—Facebook data culled from the friends of friends, looking for supporters.

The fact that the Obama campaign was able to use personal information in this way without raising the same ire as Cambridge Analytica and Facebook is a sign of how American views on technology and its role in politics have shifted over the past decade. At the time, technology was still largely viewed as a means to break traditional political structures, empower marginalized communities, and tap into the power of the grassroots. Today, however, many people have a much darker view of the role technology plays in politics—and in society as a whole. “In ’12 we talked about Obama using micro-targeting to look at your set-top box to tell you who should get what commercial, and we celebrated it,” said Zac Moffatt, who ran Mitt Romney’s digital campaign in that election. “But then we look at the next one and say, ‘Can you believe the horror of it?’ There’s an element of the lens through which you see it. To be a technology president used to be a very cool thing, and now it’s a very dangerous thing.”

DESPITE THE INNOVATIONS OF BOTH

Obama campaigns, by the time the 2016 election season rolled around, the technological advantage had shifted back to the Republicans, who had developed a sophisticated, holistic approach to digital campaigning that benefited not only Donald Trump but down-ticket Republicans as well. Republicans had access to a revamped GOP Data Center run by the party, as well as to i360, a for-profit data operation bankrolled by the Koch brothers’ network that offered incredibly detailed information on potential voters. The i360 voter files combined information purchased from commercial sources, such as shopping habits, credit status, homeownership, and religious affiliation, with voting histories, social media content, and any
connections a voter might have had with advocacy groups or other campaigns. To this, Politico reported in 2014, the Koch network added “polling, message-testing, fact-checking, advertising, media buying, [and] mastery of election law.” Democratic candidates, meanwhile, were largely beholden to the party’s official data provider, NGP VAN, with the DNC not only controlling the data, but deciding how it could be used and by whom.

The Obama team’s digital trailblazing also may have diverted attention from what the Republicans were actually up to during those years. “I think 2016 was kind of the realization that you had eight years of reporters believing everything told them by the Democratic Party—‘We know everything, and the Republicans can’t rub two rocks together,’” Moffatt said. “But if you look, the Republicans haven’t really lost since 2010, primarily based on their data fields and technology. But no one wanted to tell that story.”

One major plot-point in that story’s arc is that the Republican Party devoted more resources to social media and the internet than the Democrats did. Eighty percent of Trump’s advertising budget went to Facebook in 2016, for example. “The Trump campaign was fully willing to embrace the reality that consumption had moved to mobile, that it had moved to social,” Moffatt said. “If you think about Facebook as the entry point to the internet and a global news page, they dominated it there, while Hillary dominated all the places campaigns have historically dominated”—especially television.

Clinton’s loss hasn’t changed the basic strategy, either. Going into the midterms, Republicans continue to focus on the internet, while Democrats continue to pour money into television. (An exception is the Democratic-supporting PAC Priorities USA, which is spending $50 million on digital ads for the midterms.) Republicans are reportedly spending 40 percent on digital advertising, whereas Democrats are spending around 10 percent to 20 percent. Democratic strategist Tim Lim agrees that ignoring the internet in favor of television advertising is a flawed strategy. “The only way people can actually understand what we’re running for is if they see our messaging, and they’re not going to be seeing our messaging if we’re spending it on Wheel of Fortune and NCIS,” he said. “Democratic voters are not watching those shows.”

The Democrats are hampered by a structural problem, too: Each campaign owns its own digital tools, and when an election is over, those tools are packed up and put away. As a result, said Betsy Hoover, a veteran of both Obama campaigns who is now a partner at Higher Ground Labs, a liberal campaign-tech incubator, “four years later we’re essentially rebuilding solutions to the same problem from square one, rather than starting further up the chain.” The Republicans, by contrast, have been building platforms and seeding them up and down the party—which has allowed them to maintain their technological advantage.

“After losing in 2012, one of the most creative things the Republicans did was apply entrepreneurship to technology,” said Shomik Dutta, Hoover’s partner in Higher Ground Labs, who also worked on both Obama campaigns as well as in the Obama White House. “The Koch brothers funded i360, and the Mercers funded Cambridge Analytica and Breitbart, and they used entrepreneurship to take risks, build products, test them nimbly, and then scale up what worked quickly across the party. And that, I think, is a smart way to think about political technology.”

And so, taking a page from the Republican playbook, for the past two years Hoover and Dutta have been working to make Democrats competitive again in the arena of campaign technology. In the absence of deep-pocketed Democratic funders comparable to the Mercers and the Kochs, Higher Ground Labs acts as an incubator, looking particularly to Silicon Valley entrepreneurs to support the next generation of for-profit, election-tech startups. In 2017, the company divided $2.5 million in funding between eleven firms, and in April it announced that it was giving 13 additional startups an average of $100,000 each in seed money.

That’s still a far cry from the $50 million the Koch brothers reportedly spent to develop i360. And Higher Ground Labs faces other challenges, too. Political candidates and consultants are often creatures of habit, so getting them to try new products and untested approaches can be difficult. With presidential elections happening only every four years, and congressional elections happening every two, it can be difficult for election tech companies to sustain themselves financially. And, as has been the case with so many technology companies, growing from a small, nimble startup into a viable company that can compete on a national level is often tricky. “It’s easy to create a bunch of technology,” said Robby Mook, Hillary Clinton’s 2016 campaign manager,
“but it’s a lot harder to create technology that creates the outcomes you need at scale.”

Hoover and Dutta are hopeful that their investments in these startups will pay off. If the companies make money, Higher Ground Labs will become self-sustaining. But even if the startups fail financially, they may show what’s possible technologically. Indeed, the new tools these companies are working on are a different order of magnitude from the searchable databases that companies like Catalist pioneered just a few election cycles ago. And if they help Democratic candidates win, Hoover and Dutta view it as money well spent. “We hope to be part of the cavalry,” Hoover said.

THE COMPANIES THAT HIGHER GROUND Labs is funding are working on all aspects of campaigning: fundraising, polling, research, voter persuasion, and get-out-the-vote efforts. They show where technology—especially artificial intelligence, machine learning, and data mining—is taking campaigning, not unlike Cambridge Analytica did two years ago when it launched “psychographics” into the public consciousness. One Higher Ground-funded company has developed a platform that uses web site banner ads to measure public opinion. Another is able to analyze social media to identify content that actually changes minds (as opposed to messages that people ignore). A third has created a database of every candidate running for office across the country, providing actionable information to state party operatives and donors while building a core piece of infrastructure for the Democrats more generally.

An opposition research firm on Higher Ground’s roster, Factba.se, may offer campaigns the antidote to fake news (assuming evidence still matters in political discourse). It scours documents, social media, videos, and audio recordings to create a searchable compendium of every word published or uttered online by an individual. If you want to discover everything Donald Trump has ever said about women or steak or immigrants or cocaine, it will be in Factba.se. If you want to know every time he’s contradicted himself, Factba.se can provide that information. If you want to know just how limited his verbal skills are, that analysis is available too. (The president speaks at a fourth-grade level.) And if you want to know what’s really bugging him—or anyone—Factba.se uses software that can evaluate audio recordings and pick up on expressions of stress or discomfort in a person’s voice that are undetectable to the naked eye or ear.

To augment its targets’ dossiers, the company also uses personality tests to assess their emotional makeup. Is the subject extroverted, neurotic, depressed, or scared? Is he all of the above? (One of these tests, OCEAN—designed to measure openness, conscientiousness, extraversion, agreeableness, and neuroticism—is actually the same one that Cambridge Analytica used to construct its models.)

“We build these profiles of people based upon everything they do, and then we do an analysis,” said Mark Walsh, the CEO of Factba.se’s parent company FactSquared, who was the first chief technology officer of the Democratic Party, back in 2002. As an example, he cited the 2017 gubernatorial race in Virginia, where Ed Gillespie, the former head of the Republican National Committee, ran against Lt. Governor Ralph Northam. “We took audio and video of the three debates, and we analyzed Gillespie, looking for micro-tremors and tension in his voice when he was talking about certain topics,” Walsh said. “If you were watching the debates, you wouldn’t know that there was a huge spike when he was talking about his own party’s gun control policy, which he didn’t seem to agree with.” This was valuable intel for the Northam campaign, Walsh said—though in the end, Northam didn’t really need it. (Northam won the election by nearly nine points, the biggest margin for a Democrat in more than a quarter-century.) Still, it was a weapon that stood at the ready. “These are the types of oppo things you’re going to start to see more and more of, where candidate A will be able to fuck with the head of candidate B in ways that the populace won’t know, by saying things that they know bothers them or challenges them or makes them off-kilter,” Walsh said.

“After about 5,000 words, our AI engine can be quite predictive of what makes you happy and what makes you sad.”

“WE BUILD THESE PROFILES OF PEOPLE BASED UPON EVERYTHING THEY DO,” SAID MARK WALSH, THE CEO OF FACTSQUARED. “OUR AI ENGINE CAN BE QUITE PREDICTIVE OF WHAT MAKES YOU HAPPY AND WHAT MAKES YOU SAD.”

Judging personalities, measuring voice stress, digging through everything someone has ever said—all of this suggests that future digital campaigns, irrespective of party, will have ever-sharper tools to burrow into the psyches of candidates and voters. Consider Avalanche Strategy, another startup supported by Higher Ground Labs. Its proprietary
The manipulation of personal data to advance a political cause undermines a fundamental aspect of American democracy: the idea of a free and fair election.

algorithm analyzes what people say and tries to determine what they really mean—whether they are perhaps shading the truth or not being completely comfortable about their views. According to Michiah Prull, one of the company’s founders, the data firm prompts survey takers to answer open-ended questions about a particular issue, and then analyzes the specific language in the responses to identify “psychographic clusters” within the larger population. This allows campaigns to target their messaging even more effectively than traditional polling can—because, as the 2016 election made clear, people often aren’t completely open and honest with pollsters.

“We are able to identify the positioning, framing, and messaging that will resonate across the clusters to create large, powerful coalitions, and within clusters to drive the strongest engagement with specific groups,” Prull said. Avalanche Strategy’s technology was used by six female first-time candidates in the 2017 Virginia election who took its insights and created digital ads based on its recommendations in the final weeks of the campaign. Five of the six women won.

Clearly, despite public consternation over Cambridge Analytica’s tactics, especially in the days and weeks after Trump won (and before its data misappropriation had come to light), political campaigns are not shying away from the use of psychographics. If anything, the use of deeply personal data is becoming even more embedded within today’s approach to campaigning.

“There is real social science behind it,” Laura Quinn, the CEO of Catalist, told me not long after the 2016 election. “The Facebook platform lets people gather so much attitudinal information. This is going to be very useful in the future for figuring out how to make resource decisions about where people might be more receptive to a set of narratives or content or issues you are promoting.”

And it’s not just Facebook that provides a wealth of user information. Almost all online activity, and much offline, produces vast amounts of data that is being aggregated and analyzed by commercial vendors who sell the information to whoever will pay for it—businesses, universities, political campaigns. That is the modus operandi of what the now-retired Harvard business professor Shoshana Zuboff calls “surveillance capitalism”: Everything that can be captured about citizens is sucked up and monetized by data brokers, marketers, and companies angling for your business. That data is corralled into algorithms that tell advertisers what you might buy, insurance companies if you’re a good risk, colleges if you’re an attractive candidate for admission, courts if you’re likely to commit another crime, and on and on. Elections—the essence of our democracy—are not exempt.

Just as advertisers or platforms like Facebook and Google argue that all this data leads to ads that consumers actually want to see, political campaigns contend that their use of data does something similar: It enables an accurate ideological alignment of candidate and voter. That could very well be true. Even so, the manipulation of personal data to advance a political cause undermines a fundamental aspect of American democracy that begins to seem more remote with each passing campaign: the idea of a free and fair election. That, in the end, is the most important lesson of Cambridge Analytica. It didn’t just “break Facebook,” it broke the idea that campaigns work to convince voters that their policies will best serve them. It attempted to use psychological and other personal information to engage in a kind of voluntary disenfranchisement by depressing and suppressing turnout with messaging designed to keep voters who support the opposing candidate away from the polls—as well as using that same information to arouse fear, incite animosity, and divide the electorate.

“Manipulation obscures motive,” Prull said, and this is the problem in a nutshell: Technology may be neutral (this is debatable), but its deployment rarely is. No one cared that campaigns were using psychographics until it was revealed that psychographics might have helped put Donald Trump in the White House. No one cared about Facebook’s dark posts until they were used to discourage African Americans from showing up at the polls. No one noticed that their Twitter follower, Glenda from the heartland, with her million reasons to dislike Hillary Clinton, was really a bot created in Russia—until after the election, when the Kremlin’s efforts to use social media to sow dissension throughout the electorate were unmasked. American democracy, already pushed to the brink by unlimited corporate campaign donations, by gerrymandering, by election hacking, and by efforts to disenfranchise poor, minority, and typically Democratic voters, now must contend with a system that favors the campaign with the best data and the best tools. And as was
made clear in 2016, data can be obtained surreptitiously, and tools can be used furtively, and no one can stop it before it’s too late.

JUST AS WORRISOME AS POLITICAL CAMPAIGNS misusing technology are the outside forces seeking to influence American politics for their own ends. As Russia’s interventions in the 2016 election highlight, the biggest threats may not come from the apps and algorithms developed by campaigns, but instead from rogue operatives anywhere in the world using tools freely available on the internet.

Of particular concern to political strategists is the emerging trend of “deepfake” videos, which show real people saying and doing things they never actually said or did. These videos look so authentic that it is almost impossible to discern that they are not real. “This is super dangerous going into 2020,” Zac Moffatt said. “Our ability to process information lags behind the ability of technology to make something believable when it’s not. I just don’t think we’re ready for that.”

To get a sense of this growing threat, one only need look at a video that appeared on Facebook not long after the young Democratic Socialist Alexandria Ocasio-Cortez won her primary for a New York congressional seat in June. The video appeared to be an interview with Ocasio-Cortez conducted by Allie Stuckey, the host of Conservative Review TV, an online political channel. Stuckey, on one side of the screen, asks Ocasio-Cortez questions, and Ocasio-Cortez, on the other, struggles to respond or gives embarrassingly wrong answers. She looks foolish. But the interview isn’t real. The video was a cut-and-paste job. Conservative Review TV had taken answers from a PBS interview with Ocasio-Cortez and paired them with questions asked by Stuckey that were designed to humiliate the candidate. The effort to discredit Ocasio-Cortez was extremely effective. In less than 24 hours, the interview was viewed more than a million times.

The Ocasio-Cortez video was not especially well made; a discerning viewer could spot the manipulation. But as technology improves, deepfakes will become harder and harder to identify. They will challenge reality. They will make a mockery of federal election laws, because they will catapult viewers into a post-truth universe where, to paraphrase Orwell, power is tearing human minds to pieces and putting them together again in new shapes of someone else’s thinking.

Facebook didn’t remove the offensive Ocasio-Cortez video when it was revealed to be a fake because Stuckey claimed—after the video had gone viral—that it was satirical; the company doesn’t take down humor unless it violates its “community standards.” This and other inconsistencies in Facebook’s “fake news” policies (such as its failure to remove Holocaust denier pages) demonstrate how difficult it will be to keep bad actors from using the platform to circulate malicious information. It also reveals the challenge, if not the danger, of letting tech companies police themselves.

This is not to suggest that the government will necessarily do a better job. It is quixotic to believe that there will be a legislative intervention to regulate how campaigns obtain data and how they use it anytime soon. In September, two months before the midterm elections, Republicans in the House of Representatives pulled out of a deal with their Democratic counterparts that would have banned campaigns from using stolen or hacked material. Meanwhile, the Federal Election Commission is largely toothless, and it’s hard to imagine how routine political messages, never mind campaign tech, could be regulated, let alone if they should be. Though the government has established fair election laws in the past—to combat influence peddling and fraud, for instance—the dizzying pace at which campaign technology is evolving makes it especially difficult for lawmakers to grapple with intellectually and legislatively, and for the public to understand the stakes. “If you leave us to do this on our own, we’re gonna mess it up,” Senator Mark Warner conceded this past June, alluding to his and his colleagues’ lack of technical expertise. Instead, Warner imagined some kind of partnership between lawmakers and the technology companies they’d oversee, which of course comes with its own complications.

If there is any good news in all of this, it is that technology is also being used to expand the electorate and extend the franchise. Democracy Works, a Brooklyn-based nonprofit, for example, has partnered with Facebook on a massive effort to register new voters. And more Americans—particularly younger people—are participating in the political process through “peer-to-peer” texting apps like Hustle on the left (which initially took off during the Bernie Sanders campaign), RumbleUp on the right, and CallHub, which is nonpartisan. These mobile apps enable supporters who may not want to knock on doors or make phone calls to still engage in canvassing activities directly.

This is key, because if there is one abiding message from political consultants of all dispositions, it is that the most effective campaigns are the most intimate ones. Hacking and cheating aside, technology will only carry a candidate so far. “I think the biggest fallacy out there right now is that we win through digital,” Robby Mook said. “Campaigns win because they have something compelling to say.”

Sue Halpern is a scholar-in-residence at Middlebury College and the author, most recently, of the novel Summer Hours at the Robbers Library.