NEW AMERICA
RESILIENCE
A digital magazine exploring the boundaries of resilience

ESSAY BY DIPAYAN GHOSH

Social media and politics: Towards

Dipayan Ghosh

Dipayan Ghosh is Co-Director of the Digital Platforms & Democracy Project and Shorenstein Fellow at the Harvard Kennedy School, where he conducts economic and technology policy research on matters concerning the internet. He is also Lecturer on Law at Harvard Law School, where he teaches on the economics of internet monopolization.

electoral resilience.

Television was pivotal in bringing John Fitzgerald Kennedy to the American presidency in 1961. The candidate was charismatic, and his campaign was intelligent in how it exploited the nascent medium. But television did not merely amplify his existing characteristics, it markedly changed the tactics necessary to prevail in an election; that change in tactics entailed a change in the qualities necessary to be a credible candidate. These changes imposed by the technology on the American electorate in turn quickly reformed the nature of government itself. The nation's politics were so fundamentally shaped by television that it is now impossible to realistically imagine modern political life without it.[1]

We now have a new technological medium that joins television as a potent and central mechanism for the construction of social reality: the online communication and networking

Ghosh previously worked on global privacy and public policy issues at Facebook, where he led strategic efforts to address privacy and security. Prior, Ghosh was a technology and economic policy advisor at the White House during the Obama Administration. He served across the Office of Science & Technology Policy and the National Economic Council, where he worked on issues concerning big data's impact on consumer privacy and the digital economy. Ghosh has also served as a fellow at New America's Public Interest Technology initiative and the Open Technology Institute.

Ghosh received a PhD in electrical engineering & computer science at Cornell University, and later completed postdoctoral study in the same field at the University of California, Berkeley. His doctoral thesis examines the economic conditions under which corporates and consumers can be encouraged to adopt strong privacy standards. Ghosh holds a bachelor's degree in electrical engineering from the University of Connecticut. In 2016, *Forbes Magazine* recognized Ghosh as one of the "30 Under 30" leaders in Law & Policy.

Ghosh is the author of the forthcoming *Terms of Disservice* (Brookings Institution). His research

platforms we have come to call “social media.” The leading social media platforms exert influence both directly and in conjunction with television. “Television,” in the 1960s, comprised a small number of powerful companies: NBC, CBS, and ABC. So too “social media” today is both a technological schema and, at least with relevance to national politics, a particular and small set of services offered by an even smaller group of powerful corporations: Facebook, Google, and Twitter.[2]

There are intrinsic aspects to each sociotechnical system, about which neither the companies nor any putative regulator can change. With the advent of television, for example, Kennedy’s good looks gave him a natural advantage over Nixon that he wouldn’t have possessed before, regardless of how the Federal government or the networks might have regulated the airwaves. On the other hand, particular decisions taken by particular companies and by the governmental entities that regulate them play a significant role in shaping the nature of their political influence.

Just as television first became fundamental to American politics in

and writing have been cited and published widely, with recent analysis appearing in the *New York Times*, the *Washington Post*, the *Wall Street Journal*, the *Atlantic*, the *Guardian*, *Foreign Affairs*, *Harvard Business Review*, *Foreign Policy*, *TIME Magazine*, and CNN. He has also appeared on CNN, MSNBC, CNBC, NPR, and BBC.

the 1960 election, social media came of age most visibly in the 2012 presidential election, when President Barack Obama's reelection campaign used internet platforms to recruit and mobilize voters. Their efforts were particularly salient when directed towards younger Americans, something that would begin to change in the following election as more and more people began using social media.[3]

By the 2016 presidential election cycle, sophisticated audience-segmentation and ad-routing capacities became available to advertisers on the major platforms, enabling the incisive targeting of content. Donald Trump's campaign understood these capabilities well. As of the time of writing, much about the nature of social media's impact remains unclear.[4] Salient, knowable facts remain hidden from public view, largely because the industry remains unwilling to share meaningful data with public. But despite that lack of clarity, the results of the 2016 election make it possible to distill social media's effect during that election cycle with some simplicity: it was vicious.

This chapter sets out to trace the effect of social media in order to understand what it was that made it so objectionable throughout the 2016 election cycle. It then asks what should be done—and what realistically can be done—in both the immediate and distant future to vitiate negative impacts that may become apparent in future elections, and, ultimately, to catalyze any beneficial effects that social media might have. This chapter attempts to answer questions about social media and its effects on the industry of political communications. For instance, what does a media system look like that is resilient to nefarious actors who would seek to exploit it? How can our political system shape such a media system—and vice versa?

Several questions about what happened must be addressed in order to think intelligently about what ought to be done in the future. How did Donald Trump's campaign exploit social media to its political advantage? How did Russia manipulate internet platforms including Facebook, Google, and Twitter as part of an organized disinformation campaign to infiltrate American political discourse and destabilize our electoral system? What

impacts did social media have that resulted, not from deliberate attempts to manipulate it to a particular end, but that emerged organically from a novel sociotechnical system? Finding these answers will aid in developing a policy solution that can address these problems more effectively in future.

The Trump Campaign's Effectiveness over Social Media

Despite President Trump's aptitude and appreciation for Twitter, it was Facebook that was the digital media and political advertising platform of choice for the Trump campaign. While Facebook has been extensively leveraged by many political candidates in recent years, Trump's campaign engaged in novel, and, as some have indicated[5], especially alarming, tactics over the course of the 2016 presidential campaign.

Of all the hundreds of thousands of advertisements that the Trump campaign has said it disseminated, the sort that employed perhaps the most questionable tactics included those that some have described as voter-suppression efforts—many of which were focused on Donald Trump's

opponent, Democratic candidate Hillary Clinton.[6] In substance, the Trump campaign's activity in this area was no different from the actions of countless politicians throughout history. But what was functionally different in this case was the confluence of a politician untethered to established norms and the full commercial weight of modern social-media advertising behind his political advance. The Trump campaign, as far as is known at the time of writing (and pending the Justice Department's special investigation of the campaign's ties to Russian operatives), did nothing illegal. Rather, his campaign mastered modern messaging systems created by the leading internet companies[7] for commercial advertising. These systems leveraged audience segmentation and targeting using artificial intelligence, and would ultimately abet his political communication more than anything else.

Because of the lack of rules requiring transparency for political ads shared over the internet, it is difficult to independently trace content developed and spread by the Trump campaign. This is particularly true for Facebook, where much of the content spread by

the campaign included “dark ads,” which are posts paid for by the Trump campaign to be sent to micro-targeted social media audiences in such a manner that only people in the audience can view the ad in real time; otherwise, such advertisements are invisible to the rest of the electorate. Because of the campaign’s extensive use of this feature, the public lacks a repository of advertisements disseminated by the Trump campaign. It is therefore difficult to ascertain whether or not the campaign used certain suspicious tactics.[8] The campaign’s social media director, Brad Parscale denies having created or spread questionable content over such channels.[9]

On the other hand, campaign ads for Hillary Clinton were typically statements of her would-be policies that often featured everyday Americans engaging with the candidate. Further, Hillary Clinton’s digital campaign—which declined the offer of technical support provided directly by Facebook’s political sales team (contrary to Trump’s team)—focused its advertising on more traditional topics highlighting her political positions, largely on economic and social

matters.[10] The content also tells only half the story; because the Clinton campaign did not take Facebook's direct help in the way that the Trump campaign did, it is likely that the Trump campaign enjoyed far more viewership and organic spread of its content on Facebook and other digital platforms, as many, including Parscale, have argued.

Many commentators on American politics have noted the potential harms these kinds of tactics can have for society. The core issue at play is that the digital platforms are only loosely regulated in the United States.[11] [12] Federal oversight of the screening, transparency, funding, and spread of political content during election cycles is limited. The concern is that when the platform largely lacks any accountability to anyone, the advertiser likely need not be accountable for anything either. In the context of national politics, this is the type of media ecosystem that can seed further division leading to extreme partisanship that lacks a solid premise on voters actively making well-informed decisions about their personal beliefs. It is the type of media ecosystem that allows anyone—even a

political candidate who has made lewd comments and belatedly denounced fringe extremist supporters—to become popular just by triggering aggregate emotional responses amongst tens of millions of people who struggle every day. Not anyone can achieve such popularity. The medium heavily favors those willing to muddy the moral political compass in favor of short-term political success.

In the end, neither campaign appears to have done anything illegal over social media, so far as the public currently knows—but social media has nevertheless obscured the way in which we must now think about politics and elections, particularly because of the companies' lack of public accountability.[13] We must take a magnifying glass to American electioneering and cultivate a cleaner information ecosystem.

Malicious Russian Activity on Social Media

It is still unclear whether the Kremlin's chief goal through the course of the 2016 election cycle was to create chaos, to defeat Hillary Clinton, to support Donald Trump, or some

opportunistic combination of all three of these. But it is beyond dispute that the Russian government systematically and surreptitiously manipulated the average American social media user's information consumption during this period. Facebook, for instance, admitted that 126 million users may have been subjected to content promoted by purveyors of political disinformation working for the Kremlin. Google and Twitter, too, were infiltrated by the Russians to disseminate disinformation. In U.S. Senator Dianne Feinstein's words, this constituted "cyber-warfare." [14]

Feinstein's suggestion, then, is that the United States government must in some way fight back against foreign enemies. For months after President Trump's rise to power, the public wondered how the internet and new media could really be responsible for so much. Only a strewn-out smattering of corporate forensics, industry analysis, academic research, and persistent public inquiry was able to reveal the truth: that Russia had systematically penetrated the collective American psyche to drive a political sentiment that manifested itself at the national ballot in November 2016. [15]

The Russians' provable aggregate expenditure on digital media campaigns was minimal; on Facebook, for example, their total spending on advertising amounted to just $142,000. But because of the manner in which modern social media works, where the sharing and re-sharing of on- or off-platform content is free, it is highly likely that Russia's reach—as executed though the St. Petersburg-based Internet Research Agency (IRA), a digital spy operation attached to the Russian government—was far greater than the ad spend suggests. This comes to life when considering the number of American Facebook users who may have seen their content.

The IRA engaged in a concerted disinformation campaign aimed at subverting the Clinton campaign and supporting Trump. This is evidenced by the 3,500 Facebook advertisements released by Senate Democrats earlier this year, a database that has since been rigorously analyzed by a broad community of researchers and analysts. Most of the content the Russians shared attacked Hillary Clinton or praised Trump's positions by disseminating ads through account handles that appeared American in

origin. While their handling of social media was reportedly not particularly sophisticated, there is no doubt that the content itself was so viciously partisan that it was prone to be shared onward by members of the electorate for whom the content would resonate. Americans were spreading disinformation and propaganda to their fellow Americans—and they had no idea they were doing it.

This combination of content micro-targeting at audience slivers who would go on to share and re-share the content was likely very damaging to Hillary Clinton's chances. It was a set of practices that appropriated the tools the industry had created for legitimate advertisers, and instead brought them to bear for backhanded political gains.

The path to modern disinformation tactics

The prevalence of disinformation in Western political culture is no recent phenomenon. Propaganda has been employed by political leaders throughout history. Disinformation has always been constrained by the propagator's ability to control the creation of information and its flow to

the masses.[16] Using social media, that ability is greater now than ever before. Though ultimately special counsel Robert Mueller's "investigation did not establish that members of the Trump campaign conspired with the Russian government in its election interference activities,"[17] the campaign and the Russians did share the knowledge of modern social media's implicit political power. Facebook crossed the two-billion user threshold in 2017; hundreds of YouTube videos have been viewed over a billion times. These platforms allow for both scale and intimacy. Earlier media forms permitted one or the other, but never both at the same time.

The dissolution of social norms in the United States makes it an easy target for nefarious disinformation operations, foreign or domestic. As many have observed, large classes of the population, including communities living in but also beyond rural America, have for decades had their livelihoods ravaged by steady changes to a national economy that has shifted away from traditional industries like manufacturing and mining and moved into the information age, bringing the effects of globalization that come with

it. Longstanding manufacturing plants that powered regional economic strength have deteriorated or altogether shut down; well-paying jobs in industries that sustained American families for multiple generations have been lost; and people have been forced to rethink their lives and careers to maintain a source of income. Millions of Americans who have lived through these broad effects have also felt that their individual economic concerns have been wholly ignored by the economic and political elite found in pockets of the nation, including the east and west coasts. Thus, it is perhaps best to think of this divide between different segments of the American population as one manifesting itself along a combination of socioeconomic, geographic, and demographic lines as opposed to along any one vector. [18]

This deep-rooted divide between the "cultural elitists" and the rest of the nation is precisely the social juxtaposition that has been identified and exploited by the Trump campaign. So striking is the social disconnect between the two that noted commentators from America's heartland (the vast majority of which

leaned red in 2016) have rightly noted that the political elite simply do not understand the concerns of middle-America.[19] Though such division has long existed, it is without doubt that long-term failures of economic policy have exacerbated wealth disparity. This in turn has fueled the politicized differences concerning social issues—the most vocal corners of which lie on opposed sides of the socioeconomic spectrum in the United States. This is the social milieu into which Donald Trump dove and into which he and Parscale brought along their knowledge of a media ecosystem revolutionized by social media.

This sort of cultural environment is also susceptible to fake and biased content. Such content can be distributed at scale, with velocity and tremendous precision using modern internet-based engagement platforms hosted by the likes of Facebook and Google. All told, it constitutes a political-commercial regime that carries incredible social power.

Social media and modern political communications

Against the backdrop of such a fiercely divided nation, incendiary and provocative media injected into Americans' information diet can propel them to follow a particular political path. Modern attention spans are short; if a political message on its surface speaks to the voter's personal situation and story, that voter is far likelier to view the candidate favorably. In fact, this might occur even when the candidate's economic policy is not aligned with the voter's economic interest.

Modern social media platforms offer a tremendous channel over which to exploit these gaps in the national political system. Traditional media, including print newspapers, local news networks, and many television network programming outlets, are steadily losing viewership as eyeballs increasingly move to the internet.[20] Indeed, young people in this country are so attracted to the internet and the new media ecosystem it has produced that they may already have overtaken traditional media in overall influence. Further, the internet sector, including social media companies, are regulated only very lightly. Whereas older communications networks like internet

service providers and the cable networks have long been subject to the regulation by the Federal Communications Commission, internet companies to date are largely untouched by Federal enforcement, since the industry is a relatively new one that falls outside the authority granted to any Federal body besides the Federal Trade Commission (FTC).[21]

The FTC's Section 5 authority, it's primary tool for enforcement action against internet companies, only affords it the ability to bring actions against firms that have engaged in "unfair or deceptive" practices. For internet firms, this in practice means that the agency can only constrain the firm from conducting activities that violate commitments it has previously made to its users through such documents as a company privacy policy or a global statement of rights and responsibilities. Recently, the FTC initiated an action against the location data tracking firm Nomi Technologies, in which the agency found that the firm had not adequately informed data subjects about the collection and use of their location data for tertiary purposes. The FTC similarly applied its Section 5 authority in its investigations

of Facebook in light of the Cambridge Analytica revelations – ultimately pushing a $5 billion fine on the firm. [22]

The unfortunate truth is that this regulatory regime is inadequate to appropriately regulate the internet companies. Most firms in this sector, be they search giants or social media firms, engage in two key practices to make money: they collect as much data as possible on each user and then use that data to target users with advertisements. Companies like Google and Facebook have become tremendously good at this, both on- and off-platform. They use of a combination of first- and third-party web cookies (to be discussed later) and directly collect personal data both through their service and through third parties. Using these profiles comprised of these data, internet firms develop an inferred data profile for each user that includes the company's assertions about the user's interests, preferences, likes, dislikes, behaviors, and beliefs. In a typical case, these inferences can become quite specific; for instance, internet firms might be able to predict with a great deal of confidence where an individual lives, what her profession is, where she works, what kinds of

music, sports, movies, and art she prefers, what her ethnicity and religion is, whether she has a partner, and so on.[23]

These inferences drive the firm's advertising and content curation algorithms. As users load new pages, scroll the news feed, or conduct new searches, they see a digital display ad. The transactions of money and information that make this possible are many; but most critically, this sort of targeting is done in such a way as to engage the user for as long as possible on the platform and keep them scrolling, searching, and engaged. Indeed, experts have related the nature of social media to positive feedback loops, dopamine, and drug addiction; many have accordingly gone so far as to note the dangers of social media and like internet-based services for the individual's mental health, particularly for children.[24]

Beyond these two main pillars buttressing the business model behind the major internet firms, a number of other social and economic concerns raise further concern. One feature of the most sophisticated and widely-used digital advertising platforms, including those of Facebook and Google, that is

particularly concerning in the context of political interference is their reliance on ad-buying auctions. Firms like Google and Facebook have perfected their respective real-time digital advertising regimes. Their motivation, as with any other internet company, is to maximize advertising profits. As such, some might expect that these two firms would package up their ad inventories—that is, the aggregate advertising space derived from user engagement that they can offer their advertising clients—and sell it to the highest bidder in real time, be it Coca-Cola, a political campaign, or a disinformation agent. But for these firms, there is more at play than just the advertiser's willingness to pay for those couple ephemeral inches on a user's feed.

The most sophisticated internet firms have designed their advertising exchanges to place advertisements not only based on the advertiser's willingness to pay, but also on the likelihood that the ad campaign will engage the user so much so that the individual will click on it. Facebook and Google have developed processes to assess this likelihood on the fly. They use these algorithms to tremendous

effect in their advertising platforms. In practice, this means that advertisers in turn try to design ads that are likely to engage the user. This can quickly become a big problem if advertisers systematically attempt to game the internet platform's ad-gating algorithms and design ads promoting clickbait, fake news, hateful content, and other themes that are likelier to catch user attention for the wrong reasons. When combined with the fact that the expensiveness of placing ads also ranges proportionally with the targeted user's socioeconomic status, this set-up can directly implicate the national political integrity.

Another notable and related feature of modern digital advertising platforms that is especially concerning in the political context is audience segmentation. This refers to the advertising client's ability to pick and choose the individual users he or she wishes to target with an ad campaign. In the past, advertisers were been able to target consumers based on their personal interests. On Facebook, users have in fact for years been able to see the high-level interests associated with them through the company's Ad Preferences tool, which allows users to

adjust the interests attributed to them.[25] But starting in 2012, Facebook also enabled a powerful new method for targeting: the Custom Audience.[26] This feature allows clients to go into Facebook's advertising platform and upload lists of emails belonging to their customers or other associates. Facebook then trawls its own information warehouses and links the personally identifiable information uploaded by the client to its users. Once those linkages are made, advertisers are able to target their known customers with ads. For political advertisers, this type of tool can go a long way if the advertiser has access to voter databases.

But perhaps an even more powerful tool is that of what are known on Facebook as Lookalike Audiences.[27] These are created once an advertising client has created a Custom Audience, but wishes to target ads at yet more like-minded people. Imagine, for instance, that a Boston-based pet shop has developed a new line of dog food, and also possesses a list of the email addresses of all its past customers who have visited the establishment to purchase a dog, dog food, or a dog accessory. That list of email addresses

allows the pet shop to create a Custom Audience that would presumably mostly include individuals living close to the Boston area who are interested in dog-related products. The pet shop could now target them all with an ad, but provided the resources, and not much are needed, it could do one better: it could ask Facebook to create a Lookalike Audience by reaching into its databases and seeking out more users who are based in the area and interested in dog-related products, but who currently are not customers. That is, the Lookalike Audience would be comprised of users for whom the shop does not possess an email address.

Considering this tool in the political sphere, one could imagine the tremendous power it affords a political communicator that wishes to reach people it previously has not engaged with directly, but who are prone to listen to the political platform being described. As has been widely reported, associates of President Trump's campaign readily used this tactic; in particular, Brad Parscale made extensive use of Lookalike Audiences on Facebook.[28] The tactics of the Trump campaign were very clear: to target, analyze, and retarget the

President's eventual voters, often with clickbait and misleading content that nonetheless performed well in engaging American voters and drawing them into the extreme rhetoric he espoused in regard to issues like immigration, border control, and economic disparity.

These are the new tools of the political communications sector. They demand close examination and understanding by our policymakers. But the nation must also begin looking to broader trends in an ever-evolving industry and anticipate the tactics that will be most successful in the not-so-distant future.

Immediate remedies to improve the resilience of the social media system

As national elections approach, policymakers must consider what can be done to mitigate the effects of disinformation, including foreign interference but also weaker forms of misleading content shared by domestic actors. In the continued absence of any robust and broad reform to our broken political-media sphere that would likely require considerable political will and alignment in the Congress,

national politicians, advocates, and policy experts should consider what actionable steps industry can take on a voluntary basis. This begins with requiring greater transparency as many have been discussing. Other, potentially more effective, steps should also be taken.

Transparency

One of the most significant changes that the industry could pursue is greater transparency applied to digital advertising. In certain contexts, politics and elections among them, the purveyors of information deserve a degree of accountability for their decisions regarding the spread of information. Political communicators tap into social issues to appeal to the individual voter's psyche and charge the voter to make a certain decision at the ballot box. As they engage in this sort of activity, elections regulators are behooved to assure that there is no nefarious intent behind these efforts. Transparency can help, particularly if firms that publish digital advertisements commit to allowing the public—including journalists and researchers, who often can have

outsized impact in assuring campaign integrity—to have access to such transparency programs as searchable databases and open APIs featuring downloadable historical political ads.

In the digital advertising context, transparency with political ads can help. In particular, such a solution could explicitly tell users, in a visually prominent way, that an advertisement has been placed by a certain political actor: a political action committee, a political party, or the political candidate's campaign itself. Further, some group of people—whether the public or more specifically a group of third-party accountability officials deployed by, for instance, a government agency or self-regulation roundtable—could be provided with access to a searchable database of political ads that have been pushed on internet platforms over, say, the past six months. Such measures – which may have to be stipulated through hard regulations by governments – can maintain a level of accountability to political ad moderation by the industry, as slip-ups could be reported and corrected with some effectiveness. [29]

Finally, if and when firms discover organized disinformation operations at

any scale, there should be a requirement that they disclose it immediately to the public.[30] There is an implicit assumption here that internet firms, including social media companies, should actively monitor their platforms and proactively discover and investigate suspected disinformation operations; this is at the minimum an absolute must for the largest platforms, in no small part because it happens to be aligned with their commercial interests. We have seen this in the fallout from the Cambridge Analytica scandal. Any findings should be disclosed to the public as soon as they are made with some level of confidence; nothing less than the intellectual integrity of the electorate is at stake. If this is not done by the companies in an immediate fashion such that journalists can digest and report it, we risk misleading voters in an irreparable manner. Facebook, for its part, is beginning to do this as evidenced by its voluntary takedown and disclosure of accounts associated with disinformation operators in the lead-up to the 2018 midterm elections.

Transparency will not be enough to broadly eliminate the effects of disinformation. It is an indirect

solution; the impact it can have must be conveyed through the efforts of a small interested group of people who write and research about the impacts of political advertising. It is not a direct remedy to the egregious interference and disinformation of recent years.

Better Algorithms

To truly match nefarious disinformation operations with responsible and meaningful action, internet firms must develop better algorithms to detect, identify, and attribute attempts to push disinformation onto their platforms. Internet firms are already deploying like algorithms to notice and prevent dissemination of or proactively take down such content as hate speech and advertisements that include visual reference to alcohol, drugs, and nudity.[31] Efforts can be undertaken to better detect disinformation operations, too. Critically, internet platform companies typically know the geographic origins of an ad campaign; the currency used to pay for it; the requested timing of the ad delivery; the audience segments the client wishes to target; the content of the advertisement

itself, including any outside hyperlinks referenced; and various other key facts. Each of these data points sends an abstract signal about the intent of the advertiser, and given the level of sophistication with which these firms are developing advanced algorithmic technologies including machine learning and artificial intelligence systems, it is likely that the companies possess the technical expertise necessary to train algorithms that can find and flag disinformation efforts with high confidence and accuracy.

Indeed, the industry is already moving to enact such solutions, though there may be room for more aggressive development to this end by the likes of YouTube, Facebook, and Instagram, among others.[32] These companies must be mindful of the rights to free speech and political expression that are so ingrained in the fabric of the American democracy. Any algorithmic detection of policy-violating content should, if not previously found and acted upon, be sent to an employee for human review before any content is taken down. Internet firms should accordingly assure that they have the requisite group of employees to take these sorts of actions with

accountability—and indeed, some firms are moving actively to invest in staff expansions to this end.

A final near-term solution to the plague of disinformation that firms should consider is to crowdsource knowledge and opinions from their users themselves – potentially by enabling the flagging of certain forms of offending content – particularly if the firm lacks the resources or ability to expand its staff of human content moderators. Facebook recently implemented one such solution in Italy that effectively limited the effects of disinformation in that region, though it is difficult to determine exactly how much impact these crowdsourcing efforts may have had in the aggregate.[33]

The U.S. government, too, has tools at its disposal that can enable it to hold both the international community and corporate sector accountable. It should make use of these tools to the fullest extent to protect the electorate and the functioning of our democracy from further harm. The government should consider what can be done to curtail the impact of foreign disinformation operations by appealing to the global community. With regard to Russia, for

example, while formal diplomatic relations outside of the Oval Office are tenuous, in part because of Russia's now-confirmed activity to misinform American voters, the U.S. government should identify and, as needed, pursue opportunities to apply economic sanctions against the government of Russia and its network, should the Kremlin continue to deny its verified connection to organized disinformation operations.[34]

All corners of the government—from the legislature to the executive branch to local politicians and electoral administrators—should continue to pursue the industry and pressure it to make voluntary improvements to its core practices. This sort of pressure carries with it the implication that, should the industry not act voluntarily, regulation will follow through concerted government action. Senators Mark Warner, Amy Klobuchar and the late John McCain have provided the best example of this since the 2016 elections with their advocacy targeting political ad transparency in social media including platforms like Twitter and Facebook.[35] They have called on the industry to institute changes to the disclosures they make in political ads

disseminated through their platforms, primarily through introduction of the Honest Ads Act in 2017. While the bill seems unlikely to pass at the time of this writing because of extensive interest lobbying, the Senators' advocacy on this issue—and the effective backstop forced by the congressional threat of action—has compelled the leading platforms to make voluntary commitments to assuring greater transparency. This sort of meaningful oversight and public censure is much needed and constitutes an important tool in protecting the electorate from nefarious activity.

Longer-term considerations

The measures presented in the previous section are not total solutions; they are partial remedies at best. They cannot in and of themselves cure us of the disinformation problem that plagues American politics. Transparency into the origins of an ad cannot alone cease the activity of nefarious actors; algorithmic development is an ongoing process that disinformation operators will continually attempt to work around and, in certain cases, succeed;

and governmental efforts are unlikely to directly impact disinformation operations.

Earnest treatment of political disinformation pushed against the American electorate will demand a further examination and reform of the commercial phenomenon that is responsible for all the sophistication, influence, and opacity of modern propaganda: the core business model of the leading internet platforms. As discussed earlier, this comprises the creation of compelling services, the collection of personal data through them, and the development of opaque algorithms built to curate relevant content.

This commercial regime necessarily aligns the interests of the internet platform with those of the advertiser; both parties wish to see the user to continually scroll through social media content for minutes to hours on end. Doing so increases revenue impact for each, and thus their profit motives are effectively tied at the wrists like symbiotic fauna. But the fact is that the resulting system has opened the door for parasites to eat at the flesh of our democracy. These actors are, like legitimate advertisers, interested in

persuading the individual to absorb or be convinced by a certain idea and to act upon it in the real world. The only differences are that disinformation agents are not who they say they are and typically operate with ill motives. The obvious treatment, then, is to analyze and take the appropriate actions against the business model that has gotten here.

Privacy Reform

This will require comprehensive reforms in the ways that we regulate the technology sector. It will need to begin with a response to the unchecked corporate collection of our personal data and the uninhibited use of it to practically any ends the industry wishes. In other words, the individual requires a greater dose of privacy. This country has been through many battles in recent years on this matter, though significant Congressional legislation has never before been a matter of serious consideration. But the tides are fast changing given recent events.

Privacy is not about stipulating that certain types of companies can (or cannot) collect certain types of

personal data; there is never a situation in which a given individual might not wish to share or sell access to a given set of information. Instead, privacy must focus on the individual, and specifically on giving the individual rights in the face of the corporation. Indeed, some jurisdictions like the European Union explicitly offer privacy as a fundamental right to the citizen.[36] Meaningful privacy legislation for the American context must focus on offering the consumer a more comprehensive understanding of the types of data held on him or her; the right to say no to the collection of that data or its use in any given way; and the right to appeal to a public regulatory administrator in the case that privacy has been breached in a significant way.

Transparency and Competition Policy

New legislation is needed to implement consumer transparency into corporate practices, and to introduce greater competition amongst the leading social-media firms. Consumers must be empowered to better understand how this sector works and what companies

do with their data. This will entail greater transparency into the use of personal data, the operation of the business model, and the commercial and political actors who sit atop it and push content.

A select few firms dominate the consumer internet sector.[37] The resulting market concentration has contributed to industry abuse. This tremendous concentration in the market has serious and significant implications for online disinformation operations, too. Having so few companies in control of sophisticated targeting and curation algorithmic technologies simplifies the equation for disinformation operators and, more implicitly, decreases their independent incentives to police their platforms and clear them of bad activity or attribute it to bad actors. A first step in alleviating this matter is to give consumers greater rights to port their data from one service provider to another—a concept known as data portability.[38] Building atop that base, policymakers must begin to consider reforms to what is a broken competition policy regime in the United States, one that fails to adequately consider the impact of Silicon Valley on the consumer and

which must increase its capacity to bring greater action against the industry's abuses. In particular, policymakers should focus on examining how to bring greater scrutiny to internet firms seeking to pursue mergers and acquisitions; currently there is none, considering recent industry moves like Verizon's purchase of AOL, Facebook's acquisitions of WhatsApp and Instagram, or Google's purchases of DoubleClick and YouTube.[39] The sort of competition such scrutiny could instill will be important in the coming years to limit the impacts of online disinformation.

Conclusions

The remedies discussed in Congress and taken up by the industry, including those encouraging transparency in digital advertising, are a positive start. But they are, at best, tentative first steps that require more encouragement and upon which we must aggressively build. It is impossible to build a resilient electoral system without confronting the confluence of commercial practices of social media firms with political manipulation.

Something must give. It is simply not tenable to police the boundary between political and commercial activity with impartiality and vigor. The business models themselves must be changed—affecting, perhaps, the profitability of a small number of powerful companies—in order to protect the public-minded discourse necessary to the functioning of electoral democracy.

+ **View Footnotes**

You Might Also Like