Data&Society

Weaponizing the Digital Influence Machine:

The Political Perils of Online Ad Tech

Anthony Nadler, Matthew Crain, and Joan Donovan

EXECUTIVE SUMMARY

In this report, we argue that today's digital advertising infrastructure creates disturbing new opportunities for political manipulation and other forms of anti-democratic strategic communication. Ad platforms, web publishers, and other intermediaries have developed an infrastructure of data collection and targeting capacities that we call the **Digital Influence Machine.** The DIM incorporates a set of overlapping technologies for surveillance, targeting, testing, and automated decision-making designed to make advertising – from the commercial to the political – more powerful and efficient.

We argue that the use of the DIM to identify and target weak points where groups and individuals are most vulnerable to strategic influence is a form of **weaponization**. Unlike campaigns of even a decade ago, data-driven advertising allows political actors to zero in on those believed to be the most receptive and pivotal audiences for very specific messages while also helping to minimize the risk of political blowback by limiting their visibility to those who might react negatively. The various technologies and entities of the DIM cohere around three interlocking communication capacities:

- To use sprawling **systems of consumer monitoring** to develop detailed consumer profiles
- To **target customized audiences**, or publics, with strategic messaging across devices, channels, and contexts
- To **automate and optimize** tactical elements of influence campaigns, leveraging consumer data and real-time feedback to test and tweak key variables including the composition of target publics and the timing, placement, and content of ad messages

The social influence of the DIM, like all technological systems, is also largely a product of the political, economic, and social context in which it developed. We analyze three key shifts in the US media and political landscape that contextualize the use of the DIM to manipulate political activity:

- The decline of professional journalism;
- The expansion of financial resources devoted to political influence; and
- The growing sophistication of targeted political mobilization in a regulatory environment with little democratic accountability.

We document three distinct strategies that political actors currently use to weaponize the DIM:

- Mobilize supporters through identity threats;
- Divide an opponent's coalition; and
- Leverage influence techniques informed by behavioral science.

Despite this range of techniques, weaponized political ad targeting will rarely, if ever, be effective in changing individuals' deeply-held beliefs. Instead, the goals of weaponized DIM campaigns will be to amplify existing resentments and anxieties, raise the emotional stakes of particular issues or foreground some concerns at the expense of others, stir distrust among potential coalition partners, and subtly influence decisions about political behaviors (like whether to go vote or attend a rally). In close elections, if these tactics offer even marginal advantages, groups willing to engage in ethically dubious machinations may reap significant benefits.

Our research suggests that key points of intervention for mitigating harms are the technical structures, institutional policies, and legal regulations of the DIM. One significant further step companies could take would be to **categorically refuse to work with dark money groups**. Platforms could also limit weaponization by **requiring explicit, non-coercive user consent** for viewing any political ads that are part of a split-testing experiment. Future ethical guidelines for political advertising could be developed in collaboration with **independent committees representing diverse communities and stakeholders**. All of these possible steps have benefits, risks, and costs, and should be thoroughly and seriously considered by corporations, regulators, and civil society.

Whatever the future of online ad regulation, the consideration of political ads will only be one component in a larger effort to combat disinformation and manipulation. Without values like fairness, justice, and human dignity guiding the development of the DIM and a commitment to transparency and accountability underlying its deployment, such systems are antithetical to the principles of democracy.

CONTENTS

Author: Anthony Nadler; Associate Professor of Media and Communication Studies, Ursinus College; PhD, 2011, Communication Studies, University of Minnesota.

Author: Matthew Crain; Assistant Professor of Media, Journalism & Film, Miami University; PhD Communications 2013, Institute of Communications Research, University of Illinois, Urbana-Champaign.

Author: Joan Donovan; Media Manipulation/Platform Accountability Research Lead, Data & Society; PhD 2015, Sociology and Science Studies, University of California San Diego.

This report is published under Data & Society's Media Manipulation research initiative; for more information on the initiative, including focus areas, researchers, and funders, please visit https://datasociety.net/research/media-manipulation

INTRODUCTION

The 2016 election cycle was a breakthrough year for digital political advertising in more ways than one. First, there was a tremendous leap in spending on digital political advertising in the US. While outlays for broadcast television ads were down 20% in 2016 from the previous presidential cycle, online ad spending grew by an estimated 789% to top $1.4 billion.[1] Second, though US candidates have been placing ads online since the late 1990s, the 2016 election brought a jolt of controversy and public scrutiny to digital advertising, setting off major debates about how digital ad systems may be providing new opportunities for disinformation campaigns, propaganda, and other forms of media manipulation.

A flashpoint occurred in September 2017, when Facebook's chief security officer revealed the company had discovered "approximately $100,000 in ad spending from June of 2015 to May of 2017 — associated with roughly 3,000 ads linked to Russian groups trying to influence the US elections."[2] An investigation by special prosecutor Robert Mueller would later provide evidence that this Russian network – largely coordinated through an organization called the Internet Research Agency (IRA) – had spent millions of dollars on disinformation campaigns that aimed to intensify tensions across different groups of US citizens.[3] These efforts spanned multiple social media platforms and even entailed street protests organized with the help of Russian-sponsored digital ads.

In this report, we argue that today's digital advertising infrastructure creates disturbing new opportunities for political manipulation and other forms of anti-democratic strategic communication.[4] While our focus is political advertising, the digital systems political operatives rely upon have largely been put into place to attract commercial advertisers to the web. Ad platforms, web publishers, and other intermediaries have developed an infrastructure of data collection and targeting capacities that we call the **Digital Influence Machine**. The DIM incorporates a set of overlapping technologies for surveillance, targeting, testing, and automated decision-making designed to make advertising – from the commercial to the political – more

1 Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up," *Ad Age*, January 3, 2017, http://adage.com/article/media/2016-political-broadcast-tv-spend-20-cable-52/307346/.

2 Alex Stamos, "An Update on Information Operations on Facebook | Facebook Newsroom," *Facebook Newsroom* (blog), September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/.

3 UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC, […], https://www.justice.gov/file/1035477/download.

4 In this report, we focus on ways in which data-driven political advertising is accelerating threats to democracy beyond established practices in television and other media. Nonetheless, polls already show Americans are greatly dissatisfied with the negativity and influence of money in more traditional political advertising. A more robust ethical vision should be to imagine a media architecture designed to foster a more meaningful, participatory, and vibrant democratic life. Deborak Brooks Jordan, "Negative Campaigning Disliked by Most Americans," *Gallup* (blog), July 17, 2000, http://news.gallup.com/poll/2731/negative-campaigning-disliked-most-americans.aspx.

powerful and efficient. In industry parlance, the goal is to enable marketers to reach the right person with the right message at the right time.

Technology firms, digital marketers, and others who have built businesses around the expansion of the DIM have consistently told regulators and the public that data-driven, targeted ads benefit internet users just as much as advertisers.[5] They collectively argue that making advertisements "more relevant" benefits everyone. For instance, the Networked Advertising Initiative, a trade group representing digital advertising companies, claims advanced targeting "makes ads less annoying and irrelevant. Women are likely to see fewer ads about men's shaving products and younger people may see more ads about concerts than luxury cars." Ultimately, they claim, targeting renders a "more interesting and tailored online experience" for users. The claim is that the DIM simply makes advertisements more desirable for users. As David Drummond, Google's Chief Legal Officer, stated in testimony before the Senate Judiciary Committee, "Online advertising benefits consumers, promotes free speech, and helps small businesses succeed… Simply put, advertising is information, and relevant advertising is information that is useful to consumers."[6]

Yet, the DIM's capacities allow marketers to go much further than simply matching users with messages or products relevant to pre-existing interests. In addition to making advertisements ***more relevant*** to users, data-driven techniques can also be used to make users ***more pliable*** for advertisers. Business scholar Shoshana Zuboff highlights the drive to "predict and modify human behavior as a means to produce revenue and market control" as a key element of "surveillance capitalism."[7] In trade journals and other insider communications, many digital marketers openly speak of turning to behavioral science and neuroscience to identify cognitive biases in human decision patterns that can be exploited by well-timed interventions.[8] Digital scholar Safiya Noble, in her book, ***Algorithms of Oppression***, argues that this type of advertising-focused control underpins many companies' business models. Or, as she puts it: "Google creates advertising algorithms, not information algorithms."[9]

---

5 For instance, the Networked Advertising Initiative, a trade group representing digital advertising companies, claims advanced targeting "makes ads less annoying and irrelevant. Women are likely to see fewer ads about men's shaving products and younger people may see more ads about concerts than luxury cars." Ultimately, they claim, targeting renders "more interesting and tailored online experience" for users. National Advertising Initiative, "Understanding Online Advertising," accessed October 15, 2015, https://www.networkadvertising.org/understanding-online-advertising/how-does-it-benefit-me.

6 Quoted in Pablo Chavez, "Our Senate Testimony on Online Advertising and Google-DoubleClick," ***Google Public Policy Blog*** (blog), September 27, 2007, https://publicpolicy.googleblog.com/2007/09/our-senate-testimony-on-online.html.

7 For instance, see Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," ***Journal of Information Technology*** 30, no. 1 (March 1, 2015): 75–89, https://doi.org/10.1057/jit.2015.5; Anthony Nadler and Lee McGuigan, "An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing: Critical Studies in Media Communication," ***Critical Studies in Media Communication***, accessed March 19, 2018, https://nca.tandfonline.com/doi/abs/10.1080/15295036.2017.1387279#.Wq_X8OjwbIU; Tamsin Shaw, "Invisible Manipulators of Your Mind," ***The New York Review of Books***, April 20, 2017, http://www.nybooks.com/articles/2017/04/20/kahneman-tversky-invisible-mind-manipulators/.

8 Anthony Nadler and Lee McGuigan, "An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing," ***Critical Studies in Media Communication*** 35, no. 2 (March 15, 2018): 151–65, https://doi.org/10.1080/15295036.2017.1387279.

9 Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018), 38.

Legal scholar Ryan Calo argues that data-driven, targeted marketing allows marketers to develop techniques and technologies that "take advantage of a general understanding of cognitive limitations" of their targets and "uncover, and even trigger, consumer frailty at an individual level."[10] Such strategies can be designed to influence consumers in ways that directly contradict consumers' own self-interest, including inducing consumers toward higher prices. One striking example Calo offers is a marketing study that advises beauty advertisers to target women during "prime vulnerabilities moments" – especially Monday mornings – because their research found women "feel least attractive on Mondays."[11] The operating theory here is that advertisers can have more influence over a potential consumer if they can reach her at just the right moment of vulnerability.

We argue that this use of the DIM – *to identify and target weak points where groups and individuals are most vulnerable to strategic influence* – is a form of **weaponization**. We consider it weaponization whenever an advertising system is used to prioritize vulnerability over relevance.[12] Like beauty product marketers, political advertisers – those aiming to influence political discourse, sentiments around public issues, or political behaviors from voting to attending marches or calling representatives – are able to sift through data streams to identify prime points of vulnerability.[13] In such cases, users' data is turned against them in ways that flout the "more relevant" advertising rationale that industry advocates have used to push back against public criticism and regulatory oversight.

The operations of the Russian-linked IRA offer a good window into what the political weaponization of the DIM can look like. As a byproduct of pressure from the US Congress and journalists, rich detail is publicly available about IRA campaigns and their ad purchases that is not available for other political ad buyers. The IRA attempted to exacerbate tensions within both likely Democratic and likely Republican coalitions and suppress voting turnout among certain groups, including most notably young African Americans involved in racial justice activism. On Facebook, the IRA

10 Ryan Calo, "Digital Market Manipulation," *George Washington Law Review* 82, no. 4 (August 2014): 995.

11 PHD Media, "New Beauty Study Reveals Days, Times and Occasions When U.S. Women Feel Least Attractive," Cision PR Newswire, October 2, 2013, https://www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html.

12 There will, of course, be gray areas and points of contention over when exactly a campaign slips into weaponization. Our purpose here is not to draw a bright line to identify whether individual instances represent manipulative or non-manipulative uses of the DIM. Rather, we focus on system design. We consider the dangers posed by an immense technological infrastructure that so easily enables political operatives to leverage data to exploit vulnerabilities.

13 We are taking a wide-ranging approach to political advertising. This includes more than ads specifically meant to influence elections and much more ads than explicitly mentioning candidates. There are several reasons to keep a broad view of political influence campaigns over the DIM. First, even many online ads that do appear around elections and are likely intended to influence outcomes, do not explicitly mention candidates. Young Mie Kim (2016) and her colleagues collected a representative sample of over five million online, political ads running just before the 2016 election and found the preponderance of those ads did not explicitly mention candidates. Further, political advertising is not only used to influence electoral outcomes. Corporations, unions, advocacy groups, and astroturf groups also run influence campaigns to shape sentiments around specific issues or promote or deter participation in popular movements. The DIM weaponization strategies we describe in this report can be used for any of these aims. Young Mie Kim et al., "The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook," *Political Communication* (July 12, 2018): 1–27, https://doi.org/10.1080/10584609.2018.1476425.

used targeted advertising to promote fraudulent activist accounts. For example, those that targeted young African Americans began by championing Black art, Black dignity, and positive affirmations of Black community. However, as the election neared, these accounts turned toward trying to dissuade their publics from voting. Political communication scholar Young Mie Kim has analyzed ads from such accounts, an example of which demonstrates this shift in messaging:[14]

Fig. 1: Two IRA-created ads, November 2016

The ad on the left appeared on 11/01/2016 while the one of the right was sent out on Election Day, 11/08/2016. Both ads used identical targeting criteria provided by Facebook's ad platform to reach users flagged with interest categories such as African-American Civil Rights Movement (1954-68) and Malcom X. While this example focuses on one targeted group, these tactics were deployed by the IRA against a wide range of political figures and movements. Moreover, the DIM does not necessarily give advantage to any one political ideology, but it does offer ample resources for groups willing to pursue manipulative techniques.

Unlike campaigns of even a decade ago, data-driven advertising allowed the IRA to zero in on those believed to be the most receptive and pivotal audiences for very specific messages while also helping to minimize the risk of political blowback by limiting their visibility to those who might react negatively. They could also test many variants of ads and experiment with different targeting parameters. Such testing allows any campaign to ramp up investments when particular messages get optimal engagement.

14 Kim Mie Young, "Beware: Disguised as Your Community, Suspicious Groups May Target You Right Now for Election Interference Later" (Project DATA, August 8, 2018), https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/08/nonwhite-recruitment-and-suppression.Russia.Kim_.v.3.080818.pdf.

Tech companies have begun to take steps aimed at preventing foreign groups like the IRA from purchasing political ads in the US. As of September 2018, Facebook requires anyone purchasing political ads in the US to prove their identity with a verified US mailing address and government-issued ID card. Administrators are also required to include disclaimers on political ads that "accurately reflect the organization or person paying for your ads."[15] However, these disclosures often only provide meaningless organization names. This is especially true when ads are sponsored by "dark money" organizations (see p. 21) that can legally conceal the identity of donors. Moreover, domestic operatives may be just as tempted as foreign groups to weaponize data-driven advertising.

Since the 2016 election, a significant amount of research and journalism has examined online political advertising.[16] This report builds on that work by focusing on the underlying capacities of digital advertising infrastructures and how these capacities can be weaponized by political operatives to exploit audiences' vulnerabilities rather than address their interests. Part 1 sketches the political economy of the DIM and outlines its core technical capacities. Part 2 explains the contextual factors in US media and politics that enable digital advertising's political exploitation. Part 3 details specific strategies political operatives employ to turn the DIM into a tool for exploiting vulnerabilities. The conclusion discusses a number of steps that US policymakers and tech companies might take to minimize the risk that the DIM will aid political manipulation.

The notion that digital advertising is an unequivocal boon for consumers is quickly unraveling. Rather than simply providing relevant commercial messages, digital advertisers have designed open-ended systems to observe, predict, and modify behaviors and attitudes. These capacities threaten democratic communication, and if we hope to address this in a meaningful way we will need to do more than respond to individual crises. We need to generate the political will and practical steps to reform the foundation of a system – the DIM – that has been built to exert the maximum possible influence on the public.

15 Facebook Business, "Getting Authorized to Run Ads Related to Politics or Issues of National Importance," Advertiser Help Center, accessed September 9, 2018, https://www.facebook.com/business/help/208949576550051.

16 For instance, see Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet" (New America Foundation, January 23, 2018), /public-interest-technology/policy-papers/digitaldeceit/; Hamsini Sridharan and Ann Ravel, "Illuminating Dark Digital Politics" (Maplight, October 2017); Jeff Chester and Kathryn C. Montgomery, "The Role of Digital Marketing in Political Campaigns," *Internet Policy Review* 6, no. 4 (December 31, 2017), https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns; Emma L. Briant, "Cambridge Analytica and SCL – How I Peered inside the Propaganda Machine," *The Conversation*, April 17, 2018, http://theconversation.com/cambridge-analytica-and-scl-how-i-peered-inside-the-propaganda-machine-94867; Jeremy B. Merrill et al., "How Political Advertisers Target You on Facebook," ProPublica, 2018, https://projects.propublica.org/facebook-ads/; Shaw, "Invisible Manipulators of Your Mind."

1. THE DIGITAL INFLUENCE MACHINE

We use the term Digital Influence Machine to characterize contemporary digital advertising as an infrastructure, a layered assemblage of companies, technologies, and practices that enable advertisers to leverage consumer surveillance in order to better influence targeted publics. While the DIM extends far beyond a single device, we call it a "machine" because it fits the classic model of a machine—a system that's been constructed to allow its operators (advertisers) to act upon objects (targets of influence) with amplified technological force. The DIM incorporates the strategic communication services offered by digital ad platforms like Google and Facebook, advertising agencies and public relations firms, as well as specialized data and information technology companies such as data brokers, marketing clouds, and data management platforms (DMPs).[17] Collectively, these businesses provide an increasingly sophisticated toolkit for digital influence peddling, readily applicable to a broad range of objectives, whether an advertiser is pushing a consumer product, political candidate, or disinformation. Thus far, the DIM has been an open marketplace, available to anyone who wishes to try their hand, particularly those with ample resources. Mounting evidence shows that the DIM has been put to prodigious political use not only by official electoral campaigns, but also by special interest lobbies, foreign state actors, and domestic dark money groups.[18]

However, *political* advertising is just one component of the broader digital advertising industry, which has shown steady expansion for over two decades. In the US, more money is now spent on digital advertising – meaning online and mobile formats – than on any other media channel.[19] Analysts predict that more than half of global ad spending will go digital by 2020.[20] This growth is intertwined with significant investment in the technologies of the DIM. Digital display and video ads run in conjunction with an array of search keywords, promoted social media posts,

---

17 The various components of the DIM are not under the control of one central agent, but they are locked in interdependent commercial relationships within surveillance capitalism.

18 Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up," ***Ad Age***, January 3, 2017, http://adage.com/article/media/2016-political-broadcast-tv-spend-20-cable-52/307346/; Young Mie Kim et al., "The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook," Political Communication, forthcoming, https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Kim.FB_.StealthMedia.re_.3.two-colmns.041718-1.pdf; Jennifer Valentino-DeVries, "Facebook's Experiment In Ad Transparency Is Like Playing Hide and Seek," ***ProPublica***, January 31, 2018 https://www.propublica.org/article/facebook-experiment-ad-transparency-toronto-canada.

19 In 2016, US digital ad spending totaled $72.5 billion, surpassing television ($71.3 billion) for the first time. George Slefo, "Desktop and Mobile Revenue Surpasses TV for the First Time" ***Ad Age***, April 26, 2017, http://adage.com/article/digital/digital-ad-revenue-surpasses-tv-desktop-iab/308808/.

20 Peter Kafka, "2017 was the Year Digital Ad Spending Finally Beat TV," ***Recode***, December 4, 2017, https://www.recode.net/2017/12/4/16733460/2017-digital-ad-spend-advertising-beat-tv.

sponsored content, and native advertising formats, all of which can be targeted to highly specific audiences across websites, social feeds, mobile apps, and other channels.[21] These capacities are powered by a vast infrastructure for consumer surveillance, profiling, and targeted communications—all of which have been built up over the past two decades by waves of investment capital.[22]

Data-driven advertising has periodically raised privacy concerns among consumers and organizations from civil liberties to consumer advocacy groups.[23] That said, the digital advertising industry has consistently argued that targeted advertising serves the mutual benefit of both advertisers and consumers by matching consumers with ads based on their interests, while downplaying the potential costs of such practices. As a representative from the Direct Marketing Association told Congress in one of the first hearings on internet privacy, any harms associated with consumer data collection would be "minimal, and outweighed by the beneficial uses of the information, such as improving the visitor's experience through personalization."[24] This rationale of beneficent efficiency has proved generally successful – at least until recently – in dampening both public outcry and government regulation. Instead, a policy of hands-off self-regulation has flourished under the premise that digital communications infrastructures can serve the interests of advertisers and consumers simultaneously and without fundamental contradictions.[25]

Regardless of public opinion, the livelihoods of ad platforms and marketing data services companies ultimately depend on their ability to win over their principle clients: commercial and political advertisers. Digital ad companies therefore constantly work to improve the effectiveness of ad campaigns and to collect enough data about consumers to convince advertisers that their money is well spent. Fierce competition has propelled digital advertising companies to build innovative mechanisms for influencing consumers. As Google states in its marketing materials: "the best advertising captures people's attention, changes their perception, or prompts them to take action."[26] The industry's success has meant that the public's digital

---

21 Mara Einstein, B*lack Ops Advertising: Native Ads, Content Marketing, and the Covert World of the Digital Sell* (New York: OR Books, 2016).

22 Matthew Crain, "Financial Markets and Online Advertising: Reevaluating the Dotcom Bubble," ***Information, Communication & Society** 17* (2014): 371-384.

23 Colin Bennett, ***The Privacy Advocates: Resisting the Spread of Surveillance*** (Cambridge: MIT Press, 2008); Kathryn Montgomery, ***Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet*** (Cambridge: MIT Press, 2007).

24 Jerry Cerasale, Senior Vice President, Government Affairs, Direct Marketing Association, Inc July 13, 1999. ELECTRONIC COMMERCE: THE CURRENT STATUS OF PRIVACY PROTECTIONS FOR ONLINE CONSUMERS. House Commerce comm. sub-com telecom, trade, consumer protection. Serial No. 106-39.

25 Chris Hoofnagle, ***Federal Trade Commission Privacy Law and Policy*** (Cambridge University Press, 2016); Crain, Matthew. "The Limits of Transparency: Data Brokers and Commodification. New Media & Society 20, no. 1 (2018): 88-104. https://doi.org/10.1177/1461444816657096.

26 Google. Changing Channels: Building a Better Marketing Strategy to Reach Today's viewers. February 2018. https://services.google.com/fh/files/misc/changing_channels_a_marketers_guide_to_tv_and_video_advertising.pdf, 12.

experiences are increasingly framed by a cascading array of what Zeynep Tufecki calls "persuasion architectures."[27]

The various technologies and entities of the DIM cohere around three interlocking communication capacities.[28] The first is the capacity to use sprawling **systems of consumer monitoring** to develop detailed consumer profiles. The second is the capacity to **target customized audiences**, or publics, with strategic messaging across devices, channels, and contexts. The third is the capacity to **automate and optimize** tactical elements of influence campaigns, leveraging consumer data and real-time feedback to test and tweak key variables including the composition of target publics and the timing, placement, and content of ad messages. These functions are not wholly unique to the DIM. Advertisers have toiled for decades to develop such capacities in other media, including techniques of market segmentation, media planning, campaign testing and evaluation—all attempts to more efficiently define, reach, and influence target audiences.[29] However, as we show in this section, the DIM transforms these functions in both degree and kind.

SURVEILLANCE AND PROFILING

Digital advertising depends on the pervasive collection of consumer data across online and offline spaces. Ad platforms, social media, publishers, retailers, and many other entities routinely monitor consumers to the extent that maintaining privacy on the internet is nearly impossible. As cyber security expert Bruce Schneier conceded in 2013, "there are simply too many ways to be tracked."[30] In her book *Dragnet Nation*, investigative journalist Julia Angwin chronicles the indiscriminate nature of digital surveillance, where "institutions are stockpiling data about individuals at an unprecedented pace."[31] The data broker Acxiom claims to possess extensive marketing databases representing 100% of US consumers and households.[32] Social media platforms are among the most prodigious hoarders of consumer information. Facebook reportedly employs a classification scheme of some 52,000 attributes to

27 Zeymep Tufecki, "We're Building a Dystopia Just to Make People Click on Ads," Ted Talk, September 2017. https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads.

28 These "capacities" are an analytical disentanglement of the many overlapping practices and technologies of digital advertising. See also Zeynep Tufecki, "Engineering the Public: Big Data, Surveillance and Computational Politics," *First Monday* 19, no 7 (2014). Retrieved from http://firstmonday.org/article/view/4901/4097.

29 Joseph Turow, *Breaking Up America: Advertisers and the New Media World* (Chicago: University of Chicago Press, 1998); Eileen Meehan, *Why TV Is Not Our Fault: Television Programming, Viewers, And Who's Really In Control* (Lanham, MD: Rowman & Littlefield, 2005).

30 Bruce Schneier, "The Internet is a Surveillance State," *Schneier on Security* (blog), March 16 2013. https://www.schneier.com/essays/archives/2013/03/the_internet_is_a_su.html.

31 Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* (Times Books, 2014), 3.

32 Acxiom, "Acxiom Data: Unparalleled Global Consumer Insights," Accessed August 10, 2018 https://d1yvewpi1aplok.cloudfront.net/wp-content/uploads/2018/04/Acxiom_Data_Overview.pdf.

categorize its 2 billion monthly active users.[33] Among the information that Facebook routinely captures are data submitted directly by users such as posts, likes, profile information and social connections, data extracted from photographs and video (including facial recognition data), and many types of behavioral data, such as when and where users log in, what devices they use, and even, for a time at least, so-called "self-censored" posts that users composed but did not actually publish.[34]

Data collection methods have evolved as companies compete over the scope and depth of their data streams and respond to growing consumer adoption of ad blocking and surveillance circumvention technologies.[35] Rather than surveying specific data collection technologies, we draw upon existing research to highlight how various layers of surveillance come together to enable consumer profiling, a core capacity of the Digital Influence Machine that helps advertisers tailor their campaigns to specific publics.[36] Surveillance data are in akin to raw materials that must be refined into profiles to become useful for influence campaigns. To accomplish this, disparate data are anchored to people and devices via unique persistent identifiers, which are then linked to profile databases. One of the longest running and perhaps best known persistent ID technologies is the HTTP cookie, which now operates alongside a range of other identifying mechanisms.[37] Persistent IDs enable advertisers to continuously update profile records with new information, which over time provides insights into consumer identities, behaviors, and attitudes.

Advertisers have even developed means to track and profile users across applications and devices.[38] Google, Facebook, and a host of other ad platforms operate distributed advertising networks in conjunction with millions of external websites and mobile applications.[39] These services, along with social plug-ins such as the "like button" enable ad platforms to append behavioral web-browsing data to their own profile databases. Whether through market transactions or affiliate partnerships, consumer data is routinely exchanged among companies in order to aggregate profile

---

33 Julia Angwin, Surya Mattu and Terry Parris Jr., "Facebook Doesn't Tell Users Everything It Really Knows About Them." ***ProPublica***, December 27, 2016. https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them; Facebook, "Facebook Reports Fourth Quarter and Full Year 2017 Results," ***Facebook Investor Relations***, January 31, 2018. https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx.

34 Sauvik Das and Adam D. I. Kramer, "Self-censorship on Facebook," ***Facebook Research***, July 2, 2013. https://research.fb.com/publications/self-censorship-on-facebook/.

35 Federal Trade Commission, ***Cross Device Tracking: An FTC Staff Report***. January 2017. https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

36 For detailed examinations of data collection see: Dipayan Ghosh and Ben Scott, "#Digital Deceit: The Technologies Behind Precision Propaganda on the Internet" New America Foundation, January 2018; Wolfie Christl, "How Companies Use Personal Data Against People." Cracked Labs, October 2017, http://crackedlabs.org/en/data-against-people.

37 Jessica Davies, "WTF is a Persistent ID," ***Digiday***, March 8, 2017. https://digiday.com/marketing/wtf-persistent-id/.

38 Federal Trade Commission, ***Cross Device Tracking***.

39 Google's ad networks place tracking cookies on over three quarters of the web's one million most-visited sites. See Steven Engelhardt and Arvind Narayanan, "Online Tracking: A 1-million-site Measurement and Analysis." October 27, 2016. http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

information and facilitate targeted ad placement. A study of one million popular websites found that nearly nine in ten share data with external "third parties" of which users are most likely unaware.[40]

Data brokers like Acxiom, Experian, and Oracle enable advertisers to combine profile data obtained from various online and offline contexts.[41] Synthesizing a wide range of records from retail purchase histories to census data, Oracle Data Cloud provides an estimated 350 unique data types to Facebook to help the platform augment its profile database.[42] Nation Builder, a politically focused data management platform, which has worked with clients from local GOP parties to Emmanuel Macron, offers a "social matching" service that links email addresses to social media profile information.[43]

Building on observed actions and self-reported preferences, digital advertisers use data modeling techniques to generate further inferences and predictions about consumer attributes and behaviors. Modeling is used to fill in missing profile information, when, for example, a data broker uses ZIP code and name to extrapolate ethnicity attributes, or home ownership and education to derive political affiliation.

Building on observed actions and self-reported preferences, digital advertisers use data modeling techniques to generate further inferences and predictions about consumer attributes and behaviors. Modeling is used to fill in missing profile information, when, for example, a data broker uses ZIP code and name to extrapolate ethnicity attributes, or home ownership and education to derive political affiliation. Modeling is also used to classify consumers in numerous ways such as rating creditworthiness and determining marketing segments like "Dog Owner" or "Diabetes Interest."[44] Similarly, Facebook has patented a system that synthesizes a wide array of data points to predict "socioeconomic group classification."[45]

Digital advertisers have demonstrated particular interest in predicting consumers' "underlying psychological profiles," aiming to use such data to create psychologically

---

40 Timothy Libert. Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication* 9 (2015), 3544–3561.

41 Federal Trade Commission, Data Brokers: A Call For Transparency and Accountability, May 2014.

42 Julia Angwin, Surya Mattu and Terry Parris Jr., "Facebook Doesn't Tell Users Everything It Really Knows About Them." *ProPublica*, December 27, 2016. https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them. Oracle claims to work with over 1,500 data partners to sell access to some five million unique global consumer profiles. See Oracle, "Products: Third Party Data Audiences," Accessed March 22, 2018. https://www.oracle.com/applications/customer-experience/data-cloud/third-party-data.html.

43 nationbuilder.com.

44 Federal Trade Commission, Data Brokers, iv, v.

45 Brenden M. Sullivan et al. "Socioeconomic Group Classification Based on User Features." U.S. Patent 20180032883 filed July 27, 2016. http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180032883%22.PGNR.&OS=DN/20180032883&RS=DN/20180032883.

customized influence campaigns.[46] In a highly publicized 2013 study, researchers were able to divine a range of sensitive personal attributes using only Facebook "Likes."[47] Personality traits, political and religious views, intelligence, happiness, sexual orientation: All were predicted with high accuracy. A follow-up study found computational derivation of personality traits based on people's digital footprints to be more accurate than judgments made by friends, colleagues, and family members.[48] As one headline put it: "Facebook knows you better than your mom."[49]

TARGETING

Individual profiles are grouped into addressable publics through a variety of targeting mechanisms. Such targeting involves both audience composition (determining who sees a particular message) and ad placement (determining when and where particular ads are shown).

Facebook's full-service ad platform illustrates key elements of this targeting capacity. Advertisers can use Facebook Ad Manager to select targeting criteria from a series of dropdowns, choosing from among many thousands of possible attributes. In another variation, Facebook's Custom Audience function allows advertisers to reach more specific groups by uploading a list of identifying information, enabling, for example, voter records to be loaded as a preassembled audience. Similarly, Facebook's Lookalike Audience feature "clones" audiences that share certain attributes with targeted publics. Publics created in these ways might be: women commuters in the market for a fuel-efficient car, or registered voters in Michigan's Fifth Congressional District who share traits with guns-rights activists. While targeting based on sensitive attributes such as ethnic affinity has come under recent scrutiny for enabling discriminatory practices, researchers have found that even when platforms limit options to target sensitive categories, advertisers can still target these groups by proxy.[50]

---

46 Christopher Graves and Sandra Matz, "What Marketers Should Know About Personality-Based Marketing," ***Harvard Business Review***, May 2, 2018, https://hbr.org/2018/05/what-marketers-should-know-about-personality-based-marketing.

47 Digital records of behavior expose personal traits. Michal Kosinski, David Stillwell, Thore Graepel. *Proceedings of the National Academy of Sciences* Apr 2013, 110 (15) 5802-5805; DOI: 10.1073/pnas.1218772110.

48 Wu Youyou, Michal Kosinski, and David Stillwell, "Computer-Based Personality Judgments Are More Accurate Than Those Made By Humans," *Proceedings of the National Academy of Sciences of the United States of America* 112, no. 4 (January 27, 2015): 1036-1040. http://www.pnas.org/content/112/4/1036.full.

49 Abigail Wise, Research Says Facebook Knows You Better Than Your Mom, ***Real Simple***, (n.d.) https://www.realsimple.com/health/preventative-health/facebook-and-personality.

50 Julia Angwin and Terry Parris Jr., "Facebook Lets Advertisers Exclude Users by Race," ***ProPublica,*** October 28, 2016, https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; Spiecer et al, "Potential for Discrimination in Online Targeted Advertising," ***Proceedings of Machine Learning Research*** 81 (2018):1–15, http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf.

Targeting that is designed to exploit personality traits has been found to be particularly effective.[51] A recent study shows that tailoring persuasive appeals to targets' psychological profiles is a successful strategy for influencing their behavior.[52] Internal documents leaked in 2017 show that Facebook claimed the ability to predict its teenage users' emotional states to give advertisers the means to reach those who feel "worthless," "insecure," and "anxious."[53] While it is difficult for outside observers to know the full extent to which these kinds of strategies have been used, there are many examples of campaigns that have operated in the spirit of psychological exploitation. In early 2018, the British Army used Facebook to run a recruitment campaign that targeted 16-year-olds in the UK around the time that standardized test results were released, typically a moment of particular unease for adolescents.[54] Some of the ads suggested that students who were disappointed in their test results might pursue a career in the army, rather than say, attend university. In 2015, anti-abortion groups employed a digital ad agency to use mobile geo-fencing targeting to send ads to women who visited Planned Parenthood and other reproductive health clinics in states across the US. The ads, which included messages such as "You have choices," were triggered via GPS location data and were served to women for up to 30 days after leaving the target area.[55] Once targeting parameters are defined for such messages, the next step is to set criteria for ad placement. A Facebook advertiser can determine whether an ad runs on Facebook, Instagram, or across any number of the company's owned services and partners. Major ad platforms maintain distribution relationships with millions of websites and mobile apps that enable advertisers to reach target publics far and wide.[56]

AUTOMATING AND OPTIMIZING

While targeting parameters can be manually configured to great detail, digital advertisers increasingly rely on automated systems to test and optimize the composition of target publics as well as the timing, placement, and even content of ad messages. As the media environment has grown more complex, the digital advertising industry has invested heavily in a range of contingency-based decision-making technologies that Dipayan Ghosh and Ben Scott summarize as "weak artificial

51 Sandra Matz and Oded Netzter, Using Big Data as a Window into Consumers' Psychology," *Current Opinion in Behavioral Sciences* 18 (2017): 7-12, https://www.sciencedirect.com/science/article/pii/S2352154617300566.

52 Sandra Matz et al. "Psychological targeting as an effective approach to digital mass persuasion," *Proceedings of the National Academy of Sciences* Nov 2017, 114 (48) 12714-12719.

53 Michael Reilly, "Is Facebook Targeting Ads at Sad Teens?" *MIT Technology Review*, May 1, 2107, https://www.technologyreview.com/s/604307/is-facebook-targeting-ads-at-sad-teens/.

54 Steven Morris, "British Army Ads Targeting 'Stressed and Vulnerable Teenagers,'" *The Guardian*, June 8 2018, https://www.theguardian.com/uk-news/2018/jun/08/british-army-criticised-for-exam-results-day-recruitment-ads.

55 Zeninjor Enwemeka, "Under Agreement, Firm Won't Target Digital Ads Around Mass. Health Clinics," *WBUR*, April 4, 2017, http://www.wbur.org/bostonomix/2017/04/04/massachusetts-geofencing-ads-settlement.

56 Steven Engelhardt and Arvind Narayanan, "Online Tracking: A 1-million-site Measurement and Analysis." October 27, 2016. http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

intelligence" systems that can "understand a narrow environment, typically with a degree of memory and computational power many orders of magnitude higher than average human intelligence."[57] Here, the DIM gives advertisers the capacity to offload key tactical decisions about campaign execution to AI systems that continuously incorporate the results of multivariate experimentation to improve performance.

Across the web and mobile platforms, an array of data exchanges, programmatic media buying, and real-time bidding systems are used to place ads and to determine whether an advertiser should spend money to reach a given consumer. Rather than preselecting a publisher or application for ad placement, advertisers can bid on the right to "find and target users with specific characteristics and behaviors, regardless of which [website], service, or device is used."[58] These systems have begun to incorporate AI to evaluate the results of large numbers of bids and impressions in order to "learn" more about which consumer attributes are the most predictive of a desired influence outcome.[59] Techniques for "content optimization" apply a similar functionality to ad messaging. Through methods like split testing (also called A/B testing), advertisers can experiment with huge variations of messaging and design to, as Adobe puts it, "test combinations in real time and find the winner faster."[60]

Campaigns can be structured to influence individual behaviors like clicks and video views, but they can also be geared to elevate a particular conversation or promote social interaction.

AI systems enable advertisers to optimize their efforts to meet particular strategic objectives. Campaigns can be structured to influence individual behaviors like clicks and video views, but they can also be geared to elevate a particular conversation or promote social interaction. For example, if an advertiser sets a Facebook campaign to optimize for "engagement," the platform prioritizes "people who are the most likely to like, share, and comment … at the lowest possible cost."[61]

New techniques allow advertisers to customize outreach to individuals based on **forecasts of their vulnerability** to different persuasion strategies.[62] Researchers have experimented with "adaptive persuasion technologies" that profile consumers based

57 Ghosh and Scott, "#Digital Deceit."

58 Christl, "Corporate Surveillance State," 46.

59 HubSpot, What is deep learning? https://blog.hubspot.com/marketing/what-is-deep-learning.

60 "A/B Testing" Adobe https://www.adobe.com/mena_en/marketing-cloud/target/ab-testing.html.

61 AdEspresso, "Optimizing your Facebook campaign objective," n.d. https://adespresso.com/guides/facebook-ads-optimization/campaign-objective/.

62 M. Kaptein, P. Markopoulos, B. de Ruyter, & E. Aarts, "Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles," *International Journal of Human-Computer Studies* 2015, 77, 38–51. https://doi.org/10.1016/j.ijhcs.2015.01.004.

on their susceptibility to various appeals and, through repeat engagements, attempt to home in on the most influential persuasion strategy for each user.[63] Full-service ad platforms and marketing data clouds bundle many of these features together, enabling advertisers to automatically optimize: 1) the composition of target publics, 2) ad placement across multiple channels and screens, 3) variations on messaging content and design, and 4) budget and timeline parameters. A Facebook promotional video explains: "Our delivery system takes into account what people want to see in the context of an advertiser's desired outcome. … [The] system matches relevant ads to the right people at the right time and is constantly learning from what advertisers share about their audience and from how people interact with ads and businesses on Facebook."[64]

Many major ad platforms and data brokers have developed dedicated services to attract political campaign and special interest ad dollars. Ad platforms have also created dedicated teams of internal staff to provide technical assistance and other services to large political spenders.

Political advertisers have, like commercial advertisers, have sharply increased spending on digital formats in recent years.[65] Estimates for the 2018 election cycle vary, but it is highly likely that hundreds of millions of digital ad dollars will be spent.[66] In response to this growing demand, ad tech companies are now expressly tuning elements of the DIM for political influence. As Jeff Chester and Kathryn C. Montgomery outline in a recent study, an "infrastructure of specialized firms, services, technologies and software systems" has emerged to facilitate US political operatives' growing use of data-driven digital marketing.[67]

Many major ad platforms and data brokers have developed dedicated services to attract political campaign and special interest ad dollars.[68] Ad platforms have also created dedicated teams of internal staff to provide technical assistance and other

63 Shlomo Berkovsky, Maurits Kaptein, Massimo Zancanaro, "Adaptivity and Personalization in Persuasive Technologies," In: R. Orji, M. Reisinger, M. Busch, A. Dijkstra, A. Stibe, M. Tscheligi (eds.): *Proceedings of the Personalization in Persuasive Technology Workshop*, Persuasive Technology 2016, Salzburg, Austria, 05-04-2016, 18.

64 https://www.facebook.com/business/help/355670007911605?helpref=faq_content.

65 Kate Kaye, "Data-Driven Targeting Creates Huge 2016 Political Ad Shift: Broadcast TV Down 20%, Cable and Digital Way Up," ***Ad Age***, January 3, 2017, http://adage.com/article/media/2016-political-broadcast-tv-spend-20-cable-52/307346/; Young Mie Kim et al., "The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook," Political Communication, forthcoming, https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Kim.FB_.StealthMedia.re_.3.two-colmns.041718-1.pdf.

66 Steve Passwaiter, "2018 Campaign Ad Spend Will be in the Billions," ***Kantar Media***, September 22 2017. https://www.kantarmedia.com/us/newsroom/km-inthenews/2018-campaign-ad-spend-will-be-in-the-billions; Todd Shields and Bill Allison, "Facebook May Not Lack For Political Ads Despite Erupting Scandals," ***Bloomberg***, March 24 2018. https://www.bloomberg.com/news/articles/2018-03-24/facebook-s-grip-on-political-ads-may-defy-stain-of-data-leak.

67 Jeff Chester and Kathryn C. Montgomery, "The Role of Digital Marketing in Political Campaigns," ***Internet Policy Review*** 6, no 4, (2017), 2.

68 Chester and Montgomery, "The Role of Digital Marketing."

services to large political spenders.[69] Among the standard offerings are pre-packaged political targeting capabilities. The data broker Experian's marketing materials describe tools for political advertisers to "encourage advocacy or influence voting behavior by interweaving demographic, psychographic, and attitudinal attributes in your ads."[70] Leading up to the 2016 election, Facebook offered 14 distinct political targeting segments ranging from Politically Engaged City Dwellers (15 million "very liberal" people whose interests include opera and Bernie Sanders) to The Great Outdoors (7.3 million "very conservative" people whose interests include the NRA and Tea Party).[71] Candidates in the 2016 presidential election made extensive use of the DIM's advanced capacities for content optimization. Donald Trump's campaign reportedly ran "50,000 to 60,000 variations of Facebook ads each day, all targeting different segments of the electorate."[72]

The Democrat and Republican national parties each maintain extensive data operations that interface directly with the digital advertising industry, giving candidates the capacity to augment voter profiles with commercial data and to target video, display, mobile, and social ads across major platforms.[73] Among the numerous specialized political data outfits that work both independently and in conjunction with official parties are Organizing for America, which spun off from Barack Obama's presidential campaign, and i360, a Koch-funded data broker that counts extensive voter profiling among its specialties.[74]

---

69 Daniel Kreiss and Shannon McGregor, "Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google with Campaigns During the 2016 U.S. Presidential Cycle," ***Political Communication*** (2017): 1-23.

70 Experian Marketing Services, "Political affiliation and beyond." December 2011. Retrieved from: https://www.experian.com/assets/marketing-services/product-sheets/das-political-data-sheet.pdf.

71 Alex Kantrowitz, "Facebook's 2016 Election Team Gave Advertisers a Blueprint to a Divided US," ***Buzzfeed***, October 30, 2017, https://www.buzzfeed.com/alexkantrowitz/facebooks-2016-election-team-gave-advertisers-a-blueprint?utm_term=.coevzVRwo#.pxk7QZ83k. At the time of this report, Facebook appears to have simplified its pre-packaged political targeting to five categories: very liberal, liberal, moderate, conservative or very conservative.

72 Julia Carrie Wong, "'It Might Work Too Well': The Dark Art of Political Advertising Online," ***The Guardian***, March 19, 2018, https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy.

73 Kate Kaye, RNC's Voter Data Provider Teams Up With Google, Facebook and Other Ad Firms. AdAge. April 15, 2016. http://adage.com/article/campaign-trail/rnc-voter-data-provider-joins-ad-firms-including-facebook/303534/.

74 Mike Allen and Kenneth P. Vogel, Inside the Koch Data Mine," ***Politico***, December 8, 2014, https://www.politico.com/story/2014/12/koch-brothers-rnc-113359.

2. HOW ONLINE ADS BECAME UNACCOUNTABLE, UNMANAGEABLE, AND UNREGULATED

The social influence of the DIM, like all technological systems, depends on how it becomes embedded in social practices and how companies, policymakers, developers, institutions, and users use it. In this section, we look at three key shifts in the US media and political landscape creating conditions that facilitate the use of the DIM to manipulate political activity: 1) the decline of professional journalism; 2) the expansion of financial resources devoted to political influence; and 3) the growing sophistication of targeted political mobilization in a regulatory environment with little democratic accountability. Approaching the problem of political manipulation through this framework suggests it is social environments and media environments – not individual gullibility or omnipotent technologies – that create opportunities for manipulative operatives to leverage power on asymmetrical playing fields.[75]

First, professional news organizations have suffered severe financial retrenchment since the early 2000s. The losses are staggering. The number of jobs in newspapers fell by more than half from 2001 to 2016, a loss of over 200,000 jobs.[76] From 2006–2014, US news organizations across all sectors (newspaper, broadcast, cable, digital, etc.) lost about a third of their revenue, as the modest gains in digital news revenues could not nearly make up for losses in legacy sectors of the news industry.[77] Cuts in reporting have been uneven, hitting some communities and industry sectors much

> **Social media has become a key resource that many citizens rely upon for putting together a day-to-day understanding of what is happening in the world.**

75 For a detailed case looking at the influence of disinformation and political manipulation campaigns as the products of sociotechnical media environments, see Alice Marwick, "Why Do People Share Fake News? A Sociotechnical Model of Media Effects – Georgetown Law Technology Review," *Georgetown Law Technology Review* 2 (2018): 474–512.

76 "Newspaper Publishers Lose over Half Their Employment from January 2001 to September 2016," Bureau of Labor Statistics, April 3, 2017, https://www.bls.gov/opub/ted/2017/mobile/newspaper-publishers-lose-over-half-their-employment-from-january-2001-to-september-2016.htm?mc_cid=e73bf40429&mc_eid=e49f1168cb.

77 Jesse Holcomb and Amy Mitchell, "The Revenue Picture for American Journalism and How It Is Changing," *Pew Research Center's Journalism Project* (blog), March 26, 2014, http://www.journalism.org/2014/03/26/the-revenue-picture-for-american-journalism-and-how-it-is-changing/.

harder than others.[78] What's more, emerging news outlets and experiments with data journalism have tended to be oriented to a privileged slice of well-educated and affluent consumers already profiled as voracious news junkies.[79] State and local journalism in much of the country has also seen some of the hardest hits.[80]

Along with the financial hemorrhaging of the news industry, trust in major media organizations is declining – albeit unevenly along partisan lines – with reported levels of trust in the media lowest among Republicans.[81] Social media has become a key resource that many citizens rely upon for putting together a day-to-day understanding of what is happening in the world. A 2017 Pew poll found that about two-thirds (67%) of Americans rely on social media, at least occasionally, for finding news. As more citizens depend on platforms like Facebook and Twitter for their vantage point on political events, the DIM provides political advertisers with novel opportunities for directly embedding content in targeted social media streams and on sites around the web.

Many researchers argue that the declining fortunes of professional journalism – both in terms of financial capital and cultural authority – has been an important factor increasing the spread of misinformation and disinformation.[82] When professional news organizations no longer play such a central role in shaping shared narratives of public life and lose at least some of their agenda-setting power, this can create a power vacuum.[83] Many agents are vying to fill that role. Such a space creates the potential for political advertisers to wrest greater control over political narratives and flows of political information.

A second factor enticing increasing investment and innovation in political advertising stems from changes in the funding of US political campaigns that have come with

---

78 Philip Napoli et al., "Assessing the Health of Local Journalism Ecosystems" (New Brunswick, N.J: Rutgers University, June 2015), http://mpii.rutgers.edu/assessing-the-health-of-local-journalism-ecosystems/; James T. Hamilton and Fiona Morgan, "Poor Information: How Economics Affects the Information Lives of Low-Income Individuals," *International Journal of Communication* 12 (2018): 19.

79 Rodney Benson, "Are Foundations the Solution to the American Journalistic Crisis?" Media Ownership Project Working Paper 2016, March 2016, http://rodneybenson.org/wp-content/uploads/Benson-Are-Foundations-the-Solution_-March-20161.pdf; Brian Creech and Anthony M Nadler, "Post-Industrial Fog: Reconsidering Innovation in Visions of Journalism's Future," *Journalism*, January 28, 2017, 1464884916689573, https://doi.org/10.1177/1464884916689573; Chris W. Anderson, "Empirical Failures: Data Journalism, Cultural Identity, and the Trump Campaign," in *Trump and the Media*, by Pablo J. Boczkowski and Zizi Papacharissi (MIT Press, 2018), 33–40.

80 Paul Farhi, "Charting the Years-Long Decline of Local News Reporting," *The Washington Post*, March 26, 2014.

81 Gallop polls have indicated a tendency toward falling trust in media over the past couple of decades, though in 2017 the poll found "Democrats' trust and confidence in the mass media to report the news "fully, accurately and fairly" has jumped from 51% in 2016 to 72% this year—fueling a rise in Americans' overall confidence to 41%. Independents' trust has risen modestly to 37%, while Republicans' trust is unchanged at 14%." Art Swift, "Democrats' Confidence in Mass Media Rises Sharply From 2016," Gallup.com, September 21, 2017, https://news.gallup.com/poll/219824/democrats-confidence-mass-media-rises-sharply-2016.aspx.

82 Richard Fletcher and Rasmus Nielsen, "People Don't Trust News Media and This Is Key to the Global Misinformation Debate," in *Understanding and Addressing the Disinformation Ecosystem* (Annenberg School of Communication, 2018), 13–17, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf?x47084; Victor Pickard, "Misinformation Society," *Public Books*, November 28, 2017, http://www.publicbooks.org/the-big-picture-misinformation-society/; Alice Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," *New York: Data & Society Research Institute*, 2017.

83 W. Russell Neuman et al., "The Dynamics of Public Attention: Agenda-Setting Theory Meets Big Data," *Journal of Communication* 64, no. 2 (April 1, 2014): 193–214, https://doi.org/10.1111/jcom.12088.

WHAT IS 'DARK MONEY'?

"Dark money" is an overarching term for money spent on political influence campaigns where the identities of large donors are concealed from the public.[1]

In many cases, dark money is funneled into particular types of legally established entities that are not required to publicly disclose donors to the Federal Election Commission (FEC). Candidates, political parties, and political action committees (PACs) are required to report to the FEC the names of all donors giving more than $200. By contrast, certain types of nonprofits – 501(c) groups (with most money coming from 501(c) 4 "social welfare" organizations) – can spend portions of their budget on political activity and accept unlimited donations from individuals, corporations, and unions without disclosing donors to the public or FEC. Dark money may also flow through limited liability corporations (LLCs) that in some states, such as Delaware, can be created without even naming a founder. Super PACs are required to publicly disclose individual donors in the same vein as traditional PACs, but they differ in that they can receive unlimited funds from political nonprofits or shell groups set up as LLCs, thus making their own funding effectively anonymous.

While dark money is often associated directly with electoral politics, it can also be used to influence political opinion and activity around particular issues and movements. This is the case with many "astroturf" groups—organizations set up by industry associations, public relations firms, or other wealthy donors but made to appear to be the work of grassroots activists. Lastly, dark money can also refer to the illegal flow of money from hidden foreign sources intended to influence elections—exemplified by the Internet Research Agency's operations in the 2016 US elections.

Legal dark money spending has risen dramatically since the early 2000s, according to the Center for Responsive Politics. The center reports that about $11.2 million was spent by dark money organizations offering no donor disclosure in federal elections for the 2000 election cycle and about $5.9 million in 2004. By contrast, such groups spent over $300 million in 2012 and over $180 million in 2016 on federal elections.[2] These numbers are based on FEC reports that account for certain types of ad spending that require disclosures, but this does not include digital adve rtising. Unlike broadcast, cable, and satellite channels, digital advertisers are not required by the FEC to publicly reveal a list of sponsors for electioneering ads. More importantly, dark money groups have not only targeted high-profile congressional and presidential elections tracked in FEC reports, but have also raised serious concerns through major investments in elections with less fanfare and media attention—including school board campaigns and judicial elections.[3]

Some conservative groups, such as the Goldwater Institute, have argued that requiring public disclosure of names of donors funding political advertising can chill free speech and lead to donor harassment.[4] Yet, even in the Supreme Court's Citizens' United decision, Anthony Kennedy, writing for the majority, upheld the reasoning of previous court decisions favoring disclosure laws. Kennedy's decision reiterated that disclaimer and disclosure laws can help citizens "make informed choices in the political marketplace" and that such benefits may outweigh potential harms for political donors.[5] On September 18, 2018, the Supreme Court refused to block a ruling by a lower court that requires 501c(4)s and other dark money groups to disclose the identities of donors when these organizations engage in certain types of political advertising. This ruling is still subject to an appeal, and it remains uncertain how the FEC will enforce it. While some transparency advocates have welcomed this decision, loopholes remain that may allow dark money groups to find ways around disclosing the identities of their donors.[6]

---

1 Focusing on only electoral spending, the Center for Responsive Politics describes dark money as "political spending meant to influence the decision of a voter, where the donor is not disclosed and the source of the money is unknown." The Center for Responsive Politics, "Dark Money Primer" (Washington, D.C), accessed August 8, 2018, https://www.opensecrets.org/dark-money.

2 The Center for Responsive Politics, "Dark Money Basics," OpenSecrets, accessed September 23, 2018, https://www.opensecrets.org/dark-money/basics?range=tot.

3 Valerie Strauss, "Dark Money Just Keeps on Coming in School Board Races," *Washington Post*, October 29, 2017, https://www.washingtonpost.com/news/answer-sheet/wp/2017/10/29/dark-money-just-keeps-on-coming-in-school-board-races/; AJ Vicens, "How Dark Money Is Taking Over Judicial Elections," *Mother Jones*, October 28, 2014, https://www.motherjones.com/politics/2014/10/judicial-elections-dark-money/.

4 "'Dark Money' Disclosure Laws Will Open Door to Harassment and Intimidation," Goldwater Institute (blog), accessed September 23, 2018, https://goldwaterinstitute.org/article/dark-money-disclosure-laws-will-open-door-to-harassment/.

5 Section IV part A, CITIZENS UNITED v . FEDERAL ELECTION COMMISSION (Supreme Court of the United States, January 21, 2010).

6 Michelle Ye Hee Lee, "Political Nonprofits Seek Answers after Court Decision Targeting 'Dark Money,'" *Washington Post*, September 21, 2018, https://www.washingtonpost.com/politics/political-nonprofits-seek-answers-after-court-decision-targeting-dark-money/2018/09/21/444692f6-bd3f-11e8-8792-78719177250f_story.html?utm_term=.90d12e6b597.

changes in campaign finance regulation. Since 2000, the money spent on influencing presidential and congressional election campaigns has increased every cycle.[84] The total money spent on federal elections in 2000 was just over $3 billion, while more than $6 billion was spent on each of the 2012 and 2016 elections. An extensive analysis by Demos of political donors in 2012 and 2014 shows that known large donors are overwhelmingly wealthy, White men.[85] Demos' Sean McEwlee argues that the pivotal nature of these donations in contemporary campaigns "sharply underscore[s] how the big-money system is skewing our democracy in favor of a small, homogeneous minority." Along with greater resources devoted to influencing the elections has come an ever-expanding and experimenting industry in political consulting and advertising services specializing in political influence.[86]

It is not simply that more money is being spent on political influence; it is also being spent differently.

It is not simply that more money is being spent on political influence; it is also being spent differently. A significant shift took place following the 2010 Supreme Court ruling in *Citizens United v. Federal Elections Commission*. This ruling rolled back some of the protections of the Bipartisan Campaign Reform Act of 2002. It allowed advocacy organizations to receive unlimited funds from donors and run ads directly calling for the election or rejection of a candidate, as long as these groups do not directly coordinate with a candidate's campaign.

Since *Citizens United*, the fastest growth in spending to influence elections has come from outside groups, such as SuperPACs and nonprofit organizations that can spend large portions of their budgets on political activity.[87] During the 2016 election cycle, outside groups outspent candidates and parties in the most competitive Senate races.[88] A good amount of this spending came in the form of **dark money** (see sidebar), which conceals the source of donations from the public. Political scholar Heather Gerken argues that the enormous growth of outside spending is leading to a shift of control within the political sphere away from traditional party activists and leaders. Gerken warns these trends may "push our current party system toward one

84 This cycle-over-cycle increase in real dollars accounts for the total spending by presidential and congressional candidates, political parties, and independent groups trying to influence federal elections, according to the Center for Responsive Politics. Center for Responsive Politics, "Cost of Election," OpenSecrets.org, accessed August 8, 2018, https://www.opensecrets.org/overview/cost.php.

85 Sean McElwee, "Whose Voice, Whose Choice? The Distorting Influence of the Political Donor Class in Our Big-Money Elections" (Demos, December 6, 2016), https://www.demos.org/publication/whose-voice-whose-choice-distorting-influence-political-donor-class-our-big-money-electi.

86 Adam D. Sheingate, *Building a Business of Politics: The Rise of Political Consulting and the Transformation of American Democracy* (Oxford University Press, 2016).

87 "Outside Spending," Center for Responsive Politics, 2018, https://www.opensecrets.org/outsidespending/.

88 Ian Vandewalker, "Election Spending 2016: Outside Groups Outspend Candidates and Parties in Key Senate Races" (Brennan Center for Justice, November 1, 2016), https://www.brennancenter.org/publication/election-spending-2016-outside-groups-outspend-candidates-and-parties-key-senate-races.

that is dominated by powerful groups acting outside the formal party structure"—groups she calls "shadow parties" dominated by wealthy donors.[89] As we detail in the next section, the DIM offers a particularly hospitable environment for such political actors who can hide behind anonymity to exploit the affordances of targeted messaging without fear of reputational damage.

A third environmental factor is the growing sophistication of data-driven political influence and the lax regulatory environment in which it is taking shape. An early form of a data-driven political campaign came to prominence in the 1970s with the growth of direct mail aided by computerized lists. Direct mail became a key component of political fundraising and campaigning among conservative and, later, liberal activists.[90] Direct mail targets citizens known to have specific political opinions and allows political groups to reach out for funding or support through messages that are often emotionally polarizing and alarming.[91] As Hal Malchow, a leading Democratic direct mail consultant, told author Sasha Issenberg, "nothing is better for direct mail" than "discord."[92]

Along with the growth of the DIM in the early 2000s, parties and other political organizations started to bring data-driven insights deeper into their strategic planning. Political scientists Laura Frankle and D. Sunshine Hillygus argue that data collection and new media technologies "have changed not only how candidates communicate with the public, but also whom they contact and what they are willing to say."[93] Eitan Hersh, a leading scholar of political microtargeting, documents that the available sources of data yield great influence on how campaigns perceive and attempt to mobilize voters. Among the candidates' campaigns he has analyzed, Hersh observes that data from public records has been most influential for informing their perceptions of voters and strategies for reaching them. In fact, Hersh argues, the very design of how public records are collected and shared has been significantly influenced by politicians "crafting data laws in ways that serve the needs of their

With little regulatory oversight online, groups fueled by untraceable donors and working outside of official campaigns appear to have dominated the digital political advertising landscape in 2016.

89 Heather Gerken, "The Real Problem with Citizens United: Campaign Finance, Dark Money, and Shadow Parties," *Marquette Law Review* 97, no. 4 (2014): 925.

90 Dennis W. Johnson, *Democracy for Hire: A History of American Political Consulting* (Oxford University Press, 2017), 188–203.

91 D. Sunshine Hillygus and Todd G. Shields, *The Persuadable Voter: Wedge Issues in Presidential Campaigns* (Princeton University Press, 2014); Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns* (Crown/Archetype, 2012), 48–69.

92 Issenberg, *The Victory Lab*, 55.

93 Laura Frankel and D. Sunshine Hillygus, "Niche Communication in Political Campaigns," in *The Oxford Handbook of Political Communication*, ed. Kathleen Hall Jamieson (New York, NY: Oxford University Press, 2017), 179.

campaigns."[94] Such uses of data do not always serve constituents' interests, and Hersh argues for more democratic accountability in creating public data policies.

Though much research has focused on how candidates and their official campaigns are appropriating the resources of big data and new media, outside groups are also investing in and adapting to the age of data. In an in-depth study of mostly liberal-leaning digital organizations like MoveOn and Upworthy, David Karpf shows these organizations are developing a style of "analytic activism" that depends on "digital listening without conversation" as organizations respond to behavioral data made available by digital infrastructures.[95] At its best, such organizations will be transparent with their publics about how and why they are collecting such data and allow members different types of opportunities for participation in meaningful decision-making. Yet, listening-without-conversation techniques devolve into exploitation when surreptitious data collection merely helps organizations learn how to trigger their publics to reach predetermined goals.[96]

Much less is known about how data is being put to use by dark money organizations or other outside groups operating without the ethos of transparency of those studied by Karpf.[97] In addition to a lack of access to the organizations themselves, loose regulation of digital advertising also makes it difficult to gain much insight into their digital ad operations. The Federal Communications Commission (FCC) requires that television, cable, radio, and satellite operators make available to the public, through a searchable online archive, information about requests for time for political ads. This information includes the amount of money spent and the organization purchasing or requesting to purchase the ads—which can be a significant source for watchdogs and investigators to follow dark money groups' ads. However, online ads are exempt from this rule.[98] Online ads are also exempt from the Federal Election Commission (FEC) rules regarding disclosure and disclaimers for "electioneering communications," which include all ads that target voters and express support for or against a specific political candidate near an election. Political groups are required to file disclosures with the FEC detailing spending on "electioneering communications" if they run these

94 Eitan D. Hersh, *Hacking the Electorate: How Campaigns Perceive Voters* (Cambridge University Press, 2015), 20.

95 David Karpf, "Analytic Activism and Its Limitations," *Social Media + Society* 4, no. 1 (January 1, 2018): 2056305117750718, https://doi.org/10.1177/2056305117750718.

96 Karpf also introduces a distinction between internal and external analytics that may be pertinent to the ethical questions regarding how political organizations pursue data-driven feedback on their strategic outreach. Internal analytics are collected directly by organizations, such as monitoring traffic on their own web site or direct responses to email. External analytics work through intermediaries collecting and analyzing data—like data brokers or platforms. Arguable, external analytics have more potential to be invasive because they can collect data and perform experiments on people who have not chosen to directly interact with the organization benefiting from the analytics.

97 As an example of the difficulties researchers might face looking into these groups, the investigative reporter Jane Mayer became the target of a smear and intimidation campaign while she was investigating the large (heavily dark money) donor network surrounding Charles and David Koch. Jim Dwyer, "What Happened to Jane Mayer When She Wrote About the Koch Brothers," *The New York Times*, December 21, 2017, sec. New York, https://www.nytimes.com/2016/01/27/nyregion/what-happened-to-jane-mayer-when-she-wrote-about-the-koch-brothers.html.

98 Libby Watson, "FCC Votes to Expand Transparency for Political Ads," Sunlight Foundation, January 28, 2016, https://sunlightfoundation.com/2016/01/28/fcc-votes-to-expand-transparency-for-political-ads/.

ads on television, cable, or satellite stations—but not for online ads. Online ads are also exempt from a rule that requires a disclaimer on electioneering ads that clearly identifies their sponsor.[99]

With little regulatory oversight online, groups fueled by untraceable donors and working outside of official campaigns appear to have dominated the digital political advertising landscape in 2016. Without FCC filing requirements, the only reason we know that dark money groups were extensively advertising on some of the major platforms is because of a remarkable study run by media scholar Young Mie Kim and her colleagues at the University of Wisconsin–Madison.[100] These scholars were able to analyze over 5 million Facebook ads (including Sponsored Feed Ads) during the two months leading up to the 2016 elections. A representative national sample of over 9500 Facebook users installed an ad tracking program developed by the researchers. Kim et al. found "the volume of ads run by non-FEC groups is almost *four times larger* than that of FEC-groups."[101] By non-FEC groups, Kim et al. are referring to "501(c)(3), 501(c)(4), 501(c)(6), and other charitable organizations registered to the NCCS [National Center for Charitable Statistics] or GuideStar as a tax-exempt nonprofit" as well as "astroturf" groups or other groups or non-profits "not registered with the National Center for Charitable Statistics (NCCS), GuideStar, or the FEC."[102] The donors behind all such groups are largely concealed from the public. Astroturf groups are organizations that present themselves as grassroots groups or movements, though they are "primarily conceived, created and/or funded by corporations, industry trade associations, political interests or public relations firms."[103]

Many of these techniques draw on familiar tactics that have a long history in US politics, but the DIM accelerates their reach, hones their precision, and offers the means to evade detection and penalties.

Kathleen Hall Jamieson, one of the leading historians of American campaigning, argues that historically "third-party ads have increased the amount of deceptive content parlayed to the public—a tendency likely to become more pronounced now that advertisers' messages are able to infiltrate iPods and iPads without passing

99 For a thorough review of how campaign advertising regulations apply to digital ads, see Sridharan and Ravel, "Illuminating Dark Digital Politics."

100 Young Mie Kim et al., "The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook," *Political Communication*, forthcoming, https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Kim.FB_.StealthMedia.re_.3.two-colmns.041718-1.pdf.

101 Kim et al.

102 Kim et al.

103 The Center for Media and Democracy, "Astroturf," SourceWatch, accessed September 24, 2018, https://www.sourcewatch.org/index.php/Astroturf.

through channels of mass access."[104] Yet, it is the *data-driven practices* of these groups most likely to push the ethical frontiers of the DIM about which we know the least.

We say the online advertising system is unaccountable because platform companies, journalists, researchers, and regulators are unable to see it in order to assess it. It is unmanageable because platform companies have been unable to moderate the volume of content or create consequences for advertisers that engage in deception and other manipulative practices. Lastly, it is unregulated because online content is exempt from laws that apply to broadcast. Under these conditions, the strategies of weaponization do not just proliferate, they thrive.

104 Kathleen Hall Jamieson, "Messages, Micro-Targeting, and New Media Technologies," *The Forum* 11 (October 1, 2013), https://doi.org/10.1515/for-2013-0052.

3. STRATEGIES OF WEAPONIZING THE DIGITAL INFLUENCE MACHINE

Digital advertisers and platforms have assured consumers that data-driven targeted advertising will be convenient and efficient for both users and companies by matching ads with users' existing interests and needs. As we discussed in Part 1, this rationale has served as an underpinning for developing the immense surveillance capacities of the DIM with relatively little regulatory oversight. Many critics argue that there are broad reasons to critique the data-driven advertising beyond specific manipulative uses.[105] Others focus on the dangers of commercial manipulation.[106] Here, we focus on only a specific set of concerns about how political operatives weaponize DIM capacities by using them to target vulnerabilities to influence.

> The DIM offers several advantages over other media forms for political operatives pursuing identity threat strategies. . . . The DIM allows advertisers to carefully profile and target users who are suspected to be most sensitive to particular identity threats—making it efficient and cost-effective to target many different groups with different threatening appeals.

Below we review several political strategies that rely on the DIM to identify and exploit vulnerabilities to influence. This is not a comprehensive taxonomy but an attempt to think beyond individual campaigns and consider the kinds of strategies manipulative campaigns use with access to data-driven targeting capacities. Many of these techniques draw on familiar tactics that have a long history in US politics, but the DIM accelerates their reach, hones their precision, and offers the means to evade detection and penalties.

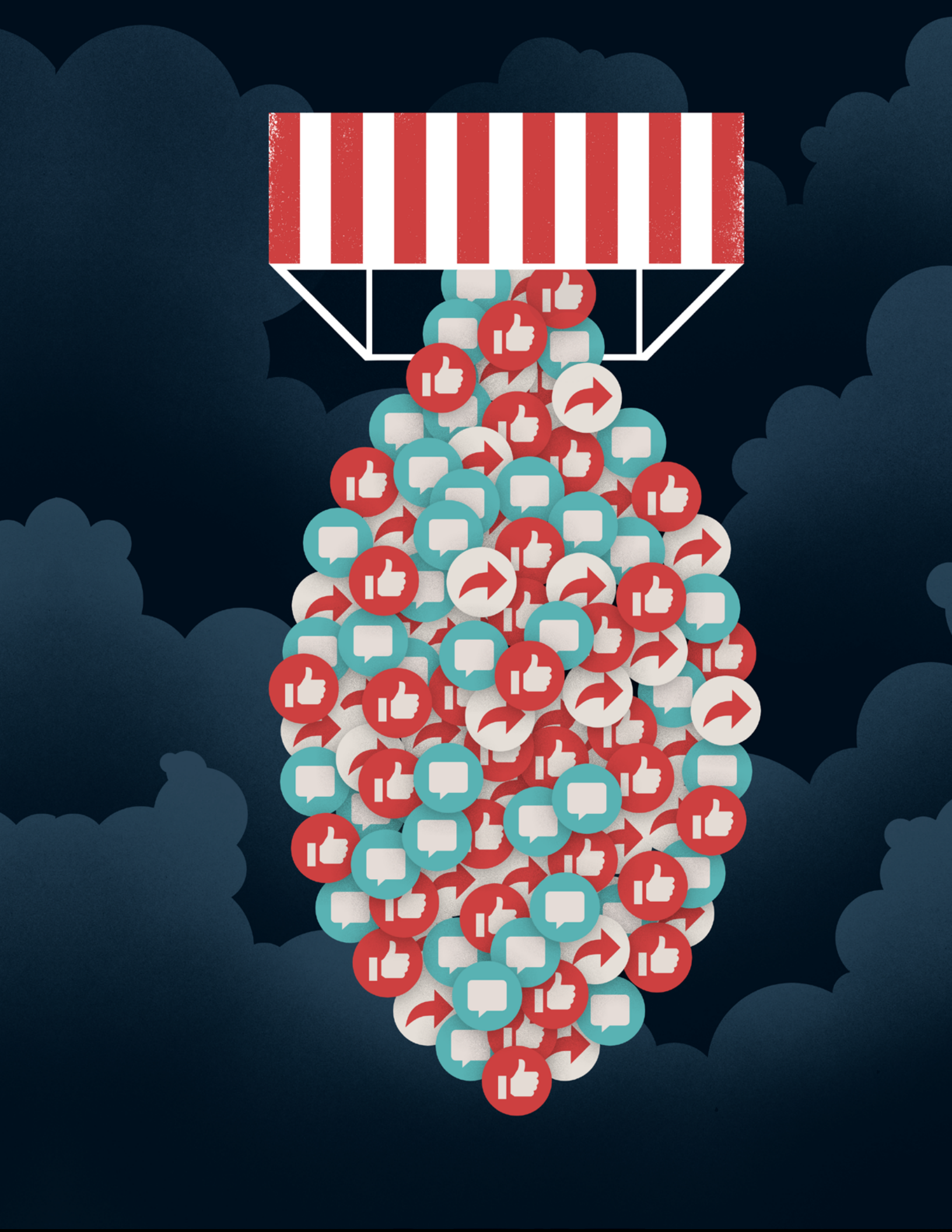
It is important to keep in mind that targeted advertising may often be one element of broader and well-coordinated digital propaganda campaigns. Such campaigns may also involve deceptive social media pages, astroturf or fake accounts, or social bots.[107] Ad

---

105 For instance, Julie Cohen argues digital surveillance generally erodes a space of privacy critical to self-discovery and development. Julie E. Cohen, "What Privacy Is For," *Harvard Law Review* 126 (2013 2012): 1904; Joe Turow argues that targeted advertising is likely to enhance class stratification and that by predicting what different categories of consumers will be interested in, then promoting products and discounts that fit those predictions, data-driven marketing will end up pushing people toward choices that match prediction models. Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven, CT: Yale University Press, 2012).

106 Calo, "Digital Market Manipulation"; Shaw, "Invisible Manipulators of Your Mind"; Nadler and McGuigan, "An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing: Critical Studies in Media Communication:"

107 Samantha Bradshaw and Phillip Howard, "Why Does Junk News Spread So Quickly Across Social Media?" (Knight Foundation, January 2018), http://comprop.oii.ox.ac.uk/research/working-papers/why-does-junk-news-spread-so-quickly-across-social-media/.



tech may also be used to channel users toward another social media page or website where further propaganda will be delivered.[108] Ads may also be used to gather lists and develop profiles of people who have responded to certain types of content.

The first two strategies we discuss below attempt to use the DIM to divide social groups by amplifying perceived threats and fears. These strategies tap into vulnerabilities that have recently come to focus in studies in political psychology on the centrality of group loyalties and social identities in political behavior. This is also a kind of social psychological model frequently discussed in military literature on "information operations."[109] The third strategy draws on cognitive psychology and a strain of behavioral science associated with behavioral economics. Together these techniques show how both individualized and group-level vulnerabilities can be exploited by political operatives.

MOBILIZE SUPPORTERS THROUGH IDENTITY THREATS

Political psychologists have increasingly come to the notion that much of popular politics revolves around sorting the world into identity groups. Individuals see themselves as belonging to these groups, and they are mobilized to action to defend or champion their group.[110] In this view, politicians, parties, and social movements compete for popular support by appealing to people's sense of group loyalty and social identity. As Christopher Achen and Larry Bartels have summarized, "group and partisan loyalties, not policy preferences or ideologies, are fundamental in democratic politics."[111] Political strategists, of course, have long intuited such pulls on people's political hearts and minds. Rallying supporters through appealing to identities and agitating anxieties around identity threats has been a timeless strategy.[112] Research suggests that one's sense of group identity tends to become more salient and mobilizing when there's a perceived identity threat – material or symbolic – posed by

108 The Russian IRA, for example, paid for some ads featuring no overt political content but rather memes relating to Pokemon, SpongeBob, BuzzFeed, and other pop culture icons. These ads targeted certain groups of teens and young adults in order to promote social media pages that mixed political messages with non-political humorous content. Alfred Ng, "'How Do You Do, Fellow Kids?' Russian Trolls Ran a Meme Page That Targeted Teens," *CNET*, May 11, 2018, https://www.cnet.com/news/russian-trolls-targeted-teens-on-facebook-with-memes/.

109 For instance, see Eric Victor Larson et al., *Understanding Commanders' Information Needs for Influence Operations* (Rand Corporation, 2009); Rod Thornton, "The Changing Nature of Modern Warfare," *The RUSI Journal* 160, no. 4 (July 4, 2015): 40–48, https://doi.org/10.1080/03071847.2015.1079047.

110 Shanto Iyengar, Gaurav Sood, and Yphtach Lelkes, "Affect, Not Ideology: A Social Identity Perspective on Polarization," *Public Opinion Quarterly* 76, no. 3 (January 1, 2012): 405–31, https://doi.org/10.1093/poq/nfs038; Leonie Huddy, Lilliana Mason, and Lene Aarøe, "Expressive Partisanship: Campaign Involvement, Political Emotion, and Partisan Identity," *American Political Science Review* 109, no. 1 (February 2015): 1–17, https://doi.org/10.1017/S0003055414000604.

111 Christopher H. Achen and Larry M. Bartels, *Democracy for Realists: Why Elections Do Not Produce Responsive Government* (Princeton University Press, 2017), 18.

112 For an in-depth study of how political campaigns can play a role in evoking "framed threats" and stimulating political anxieties, see Bethany Albertson and Shana Kushner Gadarian, *Anxious Politics: Democratic Citizenship in a Threatening World* (Cambridge University Press, 2015).

an outside group.[113] The DIM gives operatives new tools for experimenting with these strategies on different populations with greater efficiency and lower risk of damaging their own causes. Political strategists frame how to portray an opposition candidate, movement, or party as threatening or insulting to various identities, then experiment with images and storylines to make such threats vivid for their targets.

This technique can be seen in the 2016 US disinformation campaign run by the Russian IRA.[114] The identity threat strategy is clear in many of the IRA ads, such as this one targeted to Facebook accounts of Pennsylvanians who indicated "coal miner" as a job title and had interests in Donald Trump and other conservative figures (this version of the ad received 7,280 impressions with 457 clicks):

Fig. 2: IRA ad from Sept 2016 Ad ID 470

This ad further reads, "Have something against coal? Please note then that burning coal is not more harmful than lumber... You cannot leave tens of thousands of people without a job just because of lobbyists' interests." It targets a specific group with the notion that not only are powerful forces threatening their livelihood, but their self-concept and esteem are also under attack from those who dismiss their hard-work and contributions to America. This is certainly not a new or necessarily unusual tactic, though in this case we know that the IRA was targeting this occupational category to inflame an identity threat rather than represent miners' interests.

113 Cherian George captures this dynamic in a wide-ranging study of how political entrepreneurs mobilize populist-inflected and religiously fundamentalist political action across the US, India, and Indonesia. He documents a strategy – pursued with the help of social media -- that he calls "hate spin" that manufactures "vilification or indignation, used as a political strategy that exploits group identities to mobilize supporters and coerce opponents." A key to this strategy is creating a perception of status threats and insults directed against the communities being mobilized. Cherian George, *Hate Spin: The Manufacture of Religious Offense and Its Threat to Democracy* (MIT Press, 2016); For experimental research pointing to the crucial role of perceptions of outgroup threats to arousing the salience of group identity and mobilizing solidarity, see Annette R. Flippen et al., "A Comparison of Similarity and Interdependence as Triggers for In-Group Formation," *Personality and Social Psychology Bulletin* 22, no. 9 (September 1996): 882–93, https://doi.org/10.1177/0146167296229003.

114 The public has little access to records of digital political ads and targeting strategies executed by dark money groups. The set we do have most information about are those sponsored by Russian IRA accounts. Facebook provided these ads and their targeting info to Congress, then Democratic members of the House Intelligence Committee released all 3,517 ads publicly.

Another ad (3,362 impressions, 761 clicks) was targeted toward people who had liked a right-leaning, jingoistic Facebook group called "Being Patriotic," which had itself been created by the IRA:

The ad continues: "This bloody massacre is a vivid example of the fact that the war with police is too far from OVER. It's coming and the consequences will be destructive if Hillary Clinton, the main hardliner against cops, will become the president of the United States." The logic of this ad evokes an attack against the police, who are held dear by fans of "Being Patriot." Importantly, they falsely associate a horrific crime with Hillary Clinton and Black Lives Matter activism. In doing so, they increase polarization within these groups across political lines.

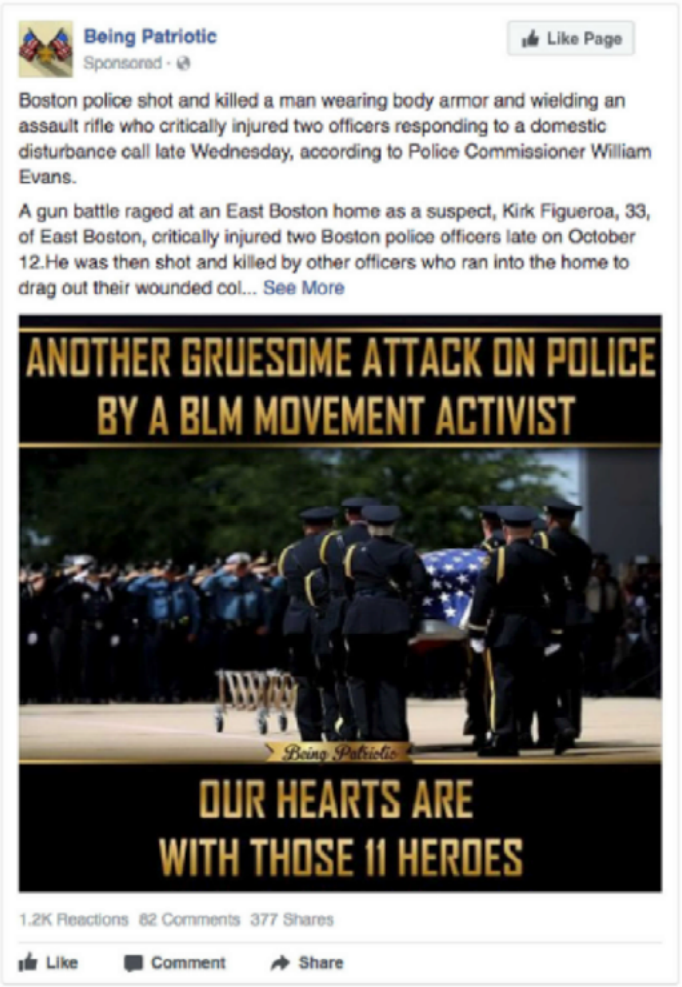


Fig. 3: IRA ad from October 2016

While identity-oriented ads predate social media, the DIM offers several advantages over other media forms for political operatives pursuing identity threat strategies. First, the DIM allows advertisers to carefully profile and target users who are suspected to be most sensitive to particular identity threats—making it efficient and cost-effective to target many different groups with different threatening appeals.

Second, the DIM helps targeted, inflammatory messages travel in an environment with few checks. Political operatives – even those working outside of official campaigns – typically have had incentive to avoid extremes in advertising venues that are not carefully "niche-ified"; research shows that negative content and attack ads can

generate backlash effects that can outweigh political gains.[115] Careful targeting can minimize such effects. Many methods of digital advertising also allow message senders to monitor how receivers are engaging with their ads—negative feedback can quickly help an advertiser adjust targeting parameters.

Targeted ads land in media spaces where their claims and messages are less likely to be challenged.

Third, targeted ads land in media spaces where their claims and messages are less likely to be challenged. The audiences for their ads are convened by the advertisers. Opposition groups have limited ability to convene the same publics for counter-message, nor do individuals receiving such messages have an ability to speak back to these publics. As Kathleen Hall Jamieson points out, microtargeting allows political advertising to operate, "without risking scrutiny and correction by reporters or scholars. Lack of critical analysis is especially problematic when such messages are pseudonymous, deceptive, un-rebutted attacks."[116] Even when targeted ads misfire or are shared beyond their initial audience, critics may have little opportunity to contest their claims or messages among the targeted audiences. Only the advertiser has access to the convened public receiving the ad.

Many of the most popular social media interfaces are designed in ways that favor the spread of content triggering quick, emotionally intense responses.

Fourth, many of the most popular social media interfaces are designed in ways that favor the spread of content triggering quick, emotionally intense responses. [117] Antonio García Martínez, who headed Facebook's early ad targeting efforts, explains that Facebook's ad system uses:

> a complex model that considers both the dollar value of each bid as well as how good a piece of clickbait (or view-bait, or comment-bait) the corresponding ad is. If Facebook's model thinks your ad is 10 times more likely to engage a user than another company's ad, then your effective bid at auction is considered 10 times higher than a company willing to pay the same dollar amount.[118]

115 Neal J. Roese and Gerald N. Sande, "Backlash Effects in Attack Politics," *Journal of Applied Social Psychology* 23, no. 8 (1993): 632–53, https://doi.org/10.1111/j.1559-1816.1993.tb01106.x; Kim L. Fridkin and Patrick J. Kenney, "Variability in Citizens' Reactions to Different Types of Negative Campaigns," *American Journal of Political Science* 55, no. 2 (2011): 307–25.

116 Hall Jamieson, "Messages, Micro-Targeting, and New Media Technologies."

117 Kerry Jones, Kelsey Libert, and Kristin Tynski, "The Emotional Combinations That Make Stories Go Viral," *Harvard Business Review*, May 23, 2016, https://hbr.org/2016/05/research-the-link-between-feeling-in-control-and-viral-content; Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press, 2018).

118 Antonio García Martínez, "How Trump Conquered Facebook Without Russian Ads," *Wired*, February 23, 2018, https://www.wired.com/story/how-trump-conquered-facebookwithout-russian-ads/.

As Michael Franz, co-director of the Wesleyan Media Project, observes, social media ad systems "incentivize campaigns to not only target their messages, but to target them in ways that would further inflame and polarize opinions."[119]

Evidence suggests these types of digital ads were most popular with third-party, political advertisers in 2016. The study of stealth advertising by Young Mie Kim and colleagues on ads run by anonymous groups demonstrated that these groups largely focused on divisive issues. The qualitative analysis performed by Kim et. al found ads run by these groups to be largely misleading, with a heavy emphasis on negative emotions and political attacks. Kim et. al also found that lower-income, White voters in swing states were most likely to be targeted by these ads, especially those dealing with immigration and race.

... also found that lower-income, White voters in swing states were most likely to be targeted by these ads, especially those dealing with immigration and race.

As political operatives develop ad tactics suited for the data-rich, digital environment, they may use these tactics in ways that go beyond the most obvious social cleavages. One can too easily imagine operators experimenting with threats targeting various identity categories – occupations, property holders, religious and ethnic groups, wedge issue publics, lifestyle segments – constantly receiving DIM feedback on what optimizes engagement and refining their approaches accordingly.

DIVIDE AN OPPONENT'S COALITION

The strategy of divide and conquer has a long history. It has been popular among union busters and economic elites seeking to splinter diverse populist coalitions through racist appeals.[120] Whenever there is a surveillance apparatus that monitors political activities and affinities, it affords opportunities to gather intelligence and exploit division. In one recent example, Energy Transfer Partners, the company constructing the Dakota Access Pipeline (DAPL), hired the security firm TigerSwan to carry out surveillance and information operations of anti-DAPL activists and organizers. An internal TigerSwan document, leaked to *The Intercept*, revealed a key recommendation: "Exploitation of ongoing native versus non-native rifts, and tribal rifts between peaceful and violent elements is critical in our effort to delegitimize the anti-DAPL movement."[121] How exactly TigerSwan pursued such goals

119 Quoted in Casey Newton, "How Facebook Rewards Polarizing Political Ads," *The Verge*, October 11, 2017, https://www.theverge.com/2017/10/11/16449976/facebook-political-ads-trump-russia-election-news-feed.

120 Michelle Alexander, *The New Jim Crow* (The New Press, 2012), 31–35.

121 Alleen Brown, Will Parrish, and Alice Speri, "Leaked Documents Reveal Counterterrorism Tactics Used at Standing Rock to 'Defeat Pipeline Insurgencies,'" *The Intercept* (blog), May 27, 2017, https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/.

we do not know, but their strategy falls in line with a long tradition of leveraging surveillance against opposing coalitions to try to stir in-fighting and promote agent provocateurs.

Political operatives are able to use the DIM to pursue this same tactic online. A senior campaign official with the Trump campaign's digital advertising team told a pair of Bloomberg reporters, "We have three major voter suppression operations underway."[122] These "voter suppression operations" were largely targeted ad campaigns designed to stir conflict among groups of Clinton voters in the effort to keep them from going to the polls. Certain African American users (profiled as "infrequent voters") were targeted with videos over Facebook to stir disgust with Clinton by playing her infamous remark about "superpredators" in praise of the mass incarceration-amplifying 1994 crime bill. Further dividing the likely Clinton coalition, certain young women were targeted with ads suggesting that Hillary Clinton herself had played a role in covering up sexual harassment and assault by her husband.

In 2016, Russian-sponsored operatives helped to organize competing rallies outside an Islamic Center in Houston, Texas. One side of this protest was organized by Heart of Texas, a Russian-organized Facebook group promoting Texas gun culture and secession.[123] This group, which had hundreds of thousands of followers, sponsored ads announcing the Houston rally while another Russian-sponsored Facebook group, United Muslims of America, promoted a rally at the same time and place—leading to a tense standoff. Russian-backed efforts to support Donald Trump's candidacy allegedly also included the use of digital advertising to break up the Democratic coalition though digital ads spreading charges that the Clinton campaign had committed fraud to defeat Bernie Sanders in the primaries.[124]

The affordances of the DIM allow political actors to sow division among opponents while also dodging accountability for such manipulations. This vulnerability is produced not just by ad tech but also by the larger apparatus of regulation and oversight on political communication. For instance, any group of motivated and sufficiently funded donors is capable of creating a so-called astroturf group—most incarnated as a "social welfare organization" designated 501(c)4 by the IRS. And crucially, 501(c)4s are not required to disclose the identity of their donors—once established, they could be getting money from essentially any source.

In the case of political division tactics, once a set of political actors have safely shielded their money behind a 501(c)4, they are able to spend money directly on political ad buying. This is where the sophisticated targeting tools of various ad

122 Joshua Green and Sasha Issenberg, "The Trump Machine is Built to Last. Bigly," *Bloomberg Businessweek*, no. 4497 (October 31, 2016): 44–49.

123 Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," *The New York Times*, February 18, 2018, sec. Politics, https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html.

124 United States of America vs. Internet Research Agency LLC, No. 18 U.S.C. §§ 2, 371, 1349, 1028A) (n.d.).

tech systems give problematic access to data-informed tools. For instance, using Facebook's standard Ad Manager interface, we were able to structure a hypothetical ad campaign targeting a worryingly specific subset of users. As you can see in Figure 4, Facebook allows the targeting of conservative women with specific interests in evangelical religion, who also have had recent anniversaries. A campaign could test messages on particular subgroups of this population, searching for techniques to drive wedges among the group. In this hypothetical case, a campaign might attempt to exploit personal data by targeting evangelical women near their anniversaries with ads that focus on candidates' alleged infidelities. While this particular example might be unlikely, the ability to produce targeted publics from some cross-cutting spheres (from the religious to the personal) allows for advertising techniques tailored to exploit this knowledge for campaigns designed to promote fractionalization.

As a campaign builds, users who engage with ads can be put on lists for future contact. Such lists can then power another round of profiling through Facebook's "lookalike" feature. This allows the campaign to start taking advantage of big data capacities as Facebook targets ads toward audiences its algorithms identify as similar to those who have already engaged with the campaign. All the while, the identity of those paying for ads are legally obscured.

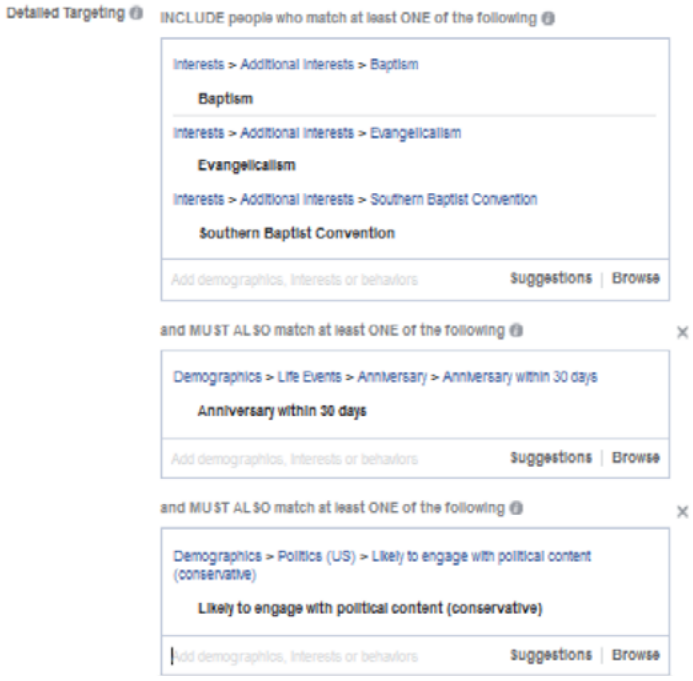


Fig. 4: Facebook Ad Manager - Image Taken 6/26/2018

Political operatives using such techniques could be looking to dissuade particular targets from voting in an upcoming election. Alternatively, such a strategy might focus on trying to stir a general sense of divisiveness and sour the political mood among a particular group. Ultimately, what this hypothetical example shows is how such actors

can make use of all of the DIM's core capacities – surveillance, profiling, targeting, and testing – for sophisticated splintering strategies.

LEVERAGE INFLUENCE TECHNIQUES INFORMED BY BEHAVIORAL SCIENCE

While digital marketers have sold the DIM to the public and regulators as a matter of matching consumers with relevant ads, many tell a different story to their clients. A growing industry of marketing services is developing sophisticated techniques for influence based on psychological models that assume psychological vulnerabilities and manipulability. [125]

For instance, Trigger Point Design claims to help "today's biggest global brands understand how behavioral psychology & decision environments work together to non-consciously drive their customers' buying behavior."[126] Irrational Labs draws on "studies how people actually act in the marketplace, as opposed to how they should or would perform if they were completely rational" in order to help devise marketing strategies.[127] Strategic Communication Labratories (SCL) – and its subsidiary Cambridge Analytica – grew out of this milieu of marketing firms interested in psychological research. After the 2016 election, Cambridge Analytica faced significant scrutiny for inappropriately using Facebook data to advance political targeting models based on psychological profiling.[128] Yet tellingly, Cambridge Analytica had received a major award for its creative use of big data on the Trump campaign from the Advertising Research Foundation, a top US trade association.[129] Combining psychological research and data-driving targeting to identify vulnerabilities is the mainstay of this field, not an outlying technique undertaken only by rogue organizations.

A growing industry of marketing services are developing sophisticated techniques for influence based on psychological models that assume psychological vulnerabilities and manipulability.

Data-driven marketers have increasingly drawn on the model of decision-making outlined by Nobel Laureate Daniel Kahneman.[130] In short, Kahneman's model (the basis of much behavioral economics) suggests humans are not rational consumers always

125 Shaw, "Invisible Manipulators of Your Mind"; Nadler and McGuigan, "An Impulse to Exploit."

126 "Behavioral Research & Design," TriggerPointDesign, accessed April 15, 2018, http://www.triggerpointdesign.com/.

127 "About Us," Irrational Labs, accessed April 15, 2018, http://irrationallabs.org/about-us/.Calo, "Digital Market Manipulation"; Shaw, "Invisible Manipulators of Your Mind"; Nadler and McGuigan, "An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing: Critical Studies in Media Communication:"

128 John Herrman, "Cambridge Analytica and the Coming Data Bust," *The New York Times*, April 15, 2018, sec. Magazine, https://www.nytimes.com/2018/04/10/magazine/cambridge-analytica-and-the-coming-data-bust.html.

129 Sapna Maheshwari, "Soul-Searching From Ad Group That Lauded Cambridge Analytica," *The New York Times*, April 18, 2018, sec. Business Day, https://www.nytimes.com/2018/03/28/business/media/cambridge-analytica-advertising-award.html.

130 Shaw, "Invisible Manipulators of Your Mind"; Calo, "Digital Market Manipulation"; Nadler and McGuigan, "An Impulse to Exploit."

maximizing their self-interest. Rather, people are always flooded by overwhelming amounts of information and rely on habits, mental shortcuts, and environmental cues. In doing so, people become, in the memorable phrase of Dan Ariely, "predictably irrational."[131] Marketers can try to intervene on that predictable irrationality.

Political campaigns draw on this research to optimize behavioral modification. Sasha Issenberg has been chronicling this arrangement for several years. In 2010, he observed that "an increasingly influential cadre of Democratic strategists" was significantly challenging the received wisdom of campaign managers through "behavioral-science experiments that treat campaigns as their laboratories and voters as unwitting guinea pigs."[132] This cadre included members of the Consortium of Behavioral Scientists, a group of unofficial advisors for the Democrats that included well-known behavioral economist and Nobel Laureate Richard Thaler.

Some political groups have started to apply social pressure and threats of shame to goad voters to go to the polls. These efforts were inspired by behavioral studies suggesting that shame could be a highly effective motivator to get out reluctant voters if they believed friends or neighbors would know if they had voted.[133] Just before a citywide election in 2017 in Los Angeles, certain residents starting receiving notifications that included their own voting history in the last three elections along with names and addresses of neighbors and acquaintances stating whether or not they had voted. The *Los Angeles Times* reported that some recipients of these letters felt harassed and violated.[134] The newspaper was unable to track down any information about the "California Voter Awareness Project," which appeared to be sending the letters. Facebook itself experimented with a massive voter mobilization study involving 61 million users and found that a "social pressure" message could increase turnout. According to the study published in *Nature*, "About 340,000 extra people turned out to vote in the 2010 US congressional elections because of a single election-day Facebook message" with the most influential messages informing users of friends who had already clicked an "I voted" button.[135]

On a webpage pitching its ad services, Google invites political advertisers to intervene upon potential voters during pivotal "micro-moments" which can "happen when

131 Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions* (Harper Collins, 2008).

132 Sasha Issenberg, "How Behavioral Science Is Remaking Politics," *The New York Times*, October 29, 2010, http://www.nytimes.com/2010/10/31/magazine/31politics-t.html.

133 Costas Panagopoulos, "Affect, Social Pressure and Prosocial Motivation: Field Experimental Evidence of the Mobilizing Effects of Pride, Shame and Publicizing Voting Behavior," *Political Behavior* 32, no. 3 (September 1, 2010): 369–86, https://doi.org/10.1007/s11109-010-9114-0.

134 Christine Mai-Duc, "A Letter Sent to Some L.A. Voters Sought to Shame Them for Their Voting Records — and No One Knows Who Sent It," *Los Angeles Times*, May 17, 2017.

135 Zoe Corbyn, "Facebook Experiment Boosts US Voter Turnout," *Nature News*, September 12, 2012, https://doi.org/10.1038/nature.2012.11401.

voters turn to a device to learn about a candidate, event, or issue."[136] Here, Google is inviting political advertisers to take on the art of using nudges and heuristics to their advantage.

With mass consumer surveillance, political advertisers can maximize the potential influence of their nudges by sifting through data to identity who is most likely to be influenced, what kinds of nudges or triggers they may be most affected by, or even factors like at what moments or in what moods a target may be most receptive.[137] For instance, political advertisers may want to test if messages promising group pride and belonging may be particularly effective when targeted toward indicators of loneliness or a recent breakup. The DIM is readymade to give them answers to such questions.

THE EFFECTS OF WEAPONIZED AD STRATEGIES

Some critics have tried to quell fears of political microtargeting by suggesting that recent reactions to the IRA and Cambridge Analytica scandals bear resemblances to moral panics surrounding propaganda and "new" media technologies of the past—like film and radio.[138] Indeed, history does show that moral panics can arise around new media technologies, especially when elites fear that ordinary people are prone to being easily manipulated by emerging media.[139]

Weaponized political ad targeting will rarely, if ever, be effective in changing individuals' deeply-held beliefs. Instead, the goals of weaponized DIM campaigns will be to amplify existing resentments and anxieties, raise the emotional stakes of particular issues or bringing to the foreground some concerns at the expense of others, stir distrust among potential coalition partners, and subtly influence decisions about ordinary behaviors (like whether to go vote or attend a rally).

The framework we offer here is quite different. As we suggest in Part 2, we should see particular media and social environments as creating conditions for manipulation, rather than blaming individual susceptibility or the irresistible force of technology. In an environment of declining professional news, surging political spending with little accountability, and lax regulation of online advertising, the design of the DIM enables political operatives

136 Kate Stanford, "How Political Ads and Video Content Influence Voter Opinion," Think with Google, March 2016, https://www.thinkwithgoogle.com/marketing-resources/content-marketing/political-ads-video-content-influence-voter-opinion/.

137 Patrick Kulp, "Ads will target your emotions and there's nothing you can do about it," Mashable, May 2, 2017. http://mashable.com/2017/05/02/facebook-ad-targeting-by-mood/.

138 For thoughtful critiques arguing fears of microtargeting have been exaggerated, see Heidi Tworek, "Cambridge Analytica, Trump, and the New Old Fear of Manipulating the Masses," *Nieman Lab* (blog), 2017, http://www.niemanlab.org/2017/05/cambridge-analytica-trump-and-the-new-old-fear-of-manipulating-the-masses/; Daniel Kreiss, "Micro-Targeting, the Quantified Persuasion," *Internet Policy Review* 6, no. 4 (December 31, 2017), https://policyreview.info/articles/analysis/micro-targeting-quantified-persuasion; Jessica Baldwin-Philippi, "The Myths of Data-Driven Campaigning," *Political Communication* 34, no. 4 (October 2, 2017): 627–33, https://doi.org/10.1080/10584609.2017.1372999.

139 A. Brad Schwartz, *Broadcast Hysteria: Orson Welles's War of the Worlds and the Art of Fake News*, Reprint edition (Place of publication not identified: Hill and Wang, 2016).

to weaponize its capacities. Yet, to think critically about the actual threats posed by DIM targeting strategies, we need to recognize that they will not render forms of mind control or magic bullets of influence. Weaponized political ad targeting will rarely, if ever, be effective in changing individuals' deeply-held beliefs. Instead, the goals of weaponized DIM campaigns will be to amplify existing resentments and anxieties, raise the emotional stakes of particular issues or bringing to the foreground some concerns at the expense of others, stir distrust among potential coalition partners, and subtly influence decisions about ordinary behaviors (like whether to go vote or attend a rally). In close elections, if these tactics offer even marginal advantages, groups willing to engage in such machinations may reap significant benefits.

While some campaigns may want to refrain from the most egregiously manipulative DIM strategies, more roguish actors may indirectly pressure others to follow their lead. Writing in trade magazine *Campaigns and Elections*, digital campaign consultant Laura Packard makes this plea to her industry:

> At the end of the day, if voters don't punish candidates for running unethical campaigns, and candidates do not punish consultants and staff for crossing the line, we can look forward to even more of it. When an entire field is 'juiced,' eventually it becomes impossible to compete fairly without steroids. Is this what we want the future of campaigning to be?[140]

140 Laura Packard, "It's Time for An Industry-Wide Conversation on Ethics," *Campaigns & Elections*, May 16, 2018, https://www.campaignsandelections.com/campaign-insider/it-s-time-for-an-industry-wide-conversation-on-ethics.

4. PROSPECTS FOR REFORMING THE DIGITAL INFLUENCE MACHINE

We conclude by considering a few possibilities for the future of the DIM. As we have shown above, advertising is a fundamental component of the contemporary internet—woven into the technical structure and business models of major platform companies. Hence, at the economic foundation of the internet as we've come to know it lies an immense apparatus of data-monitoring, profiling, message testing, and targeting designed for advertisers to exert influence. This makes advertising a crucial subject of analysis and critique. There will always be individuals and organizations intent on the manipulating the public, whether political operatives or commercial marketers. The techniques and examples described above demonstrate that such manipulations are capable of real harms at scales both large and small. Our research suggests that key points of intervention on these harms are the technical structures, institutional policies, and legal regulations of the DIM. In this section, we suggest and analyze a number of possible reforms to the infrastructure of digital advertising.

Media reform movements usually favor government regulations because, as several researchers argue, media industry self-regulation schemes often skew toward protecting businesses from criticism rather than protecting the public.

This may be a propitious moment for meaningful reform, as today the narrative of social media as inherently empowering is unraveling. Testifying before the US Senate, Facebook CEO Mark Zuckerberg admitted this:

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. . . . But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake.[141]

Zuckerberg's remarks signals an expanding recognition of the need for social and political accountability in the design of media structures so central to contemporary communication. His appearance before Congress also indicates that new government

141 Mark Zuckerberg, "Mark Zuckerberg's Wednesday Testimony to Congress on Cambridge Analytica," *Politico*, accessed July 7, 2018, https://politi.co/2GNxFLx.

regulation is one possible future for the DIM. Across many decades, media reform activists have looked to the regulatory powers of the democratic state as the best force to ensure that media meet public interest ideals and balance out concentrations of corporate power.[142] In 2018, there are signs that Congress and the FEC have taken interest in tackling the problems of political manipulation through digital advertising. The FEC has begun hearings on rule changes for online political ads, and as of July 2018, there are 30 US senators cosponsoring the "Honest Ads Act."[143] Yet, given the widespread sense of partisan gridlock in Congress and a regulatory apparatus still wedded to a deregulatory, pro-market ideology, there is little hope of major changes in the near term at the federal level. Better near-term prospects may be found at the state level. Several states, including California, Montana, Washington, and New York, have passed laws requiring greater disclosure of political spending than mandated federally.

At the same time, the federal government is lifting restrictions on the DIM. In 2017, President Trump signed a law repealing regulations that would have required internet service providers "to obtain consumer consent before using precise geolocation, financial information, health information, children's information and web-browsing history for advertising and marketing."[144] In July 2018, the Treasury Department announced it will no longer require 501(c)4 social welfare groups to report the names of large donors to the IRS. Critics says this change will make it easy for foreign funds to fuel dark money groups.[145]

There are several possible avenues for legislation that would push against the trends described above. Legislators could consider requiring all political advertisers to disclose their significant donors.[146] Regulators could also end exemptions for online ads from FEC electioneering regulations and require platforms to report the sponsors and targeting parameters of political ad purchases. Legislators could consider an overarching data privacy policy framework in the spirit of the EU General Data Protection Regulation's rights-based approach. Aiming at more structural issues, media scholar Victor Pickard has proposed taxing digital platforms to support an

142 Robert W. McChesney, *Telecommunications, Mass Media, and Democracy: The Battle for the Control of U.S. Broadcasting, 1928-1935* (New York : Oxford University Press, 1993); Victor Pickard, *America's Battle for Media Democracy: The Triumph of Corporate Libertarianism and the Future of Media Reform* (New York: Cambridge University Press, 2014).

143 This is a modest bill that would require similar disclosures from online political ads as for television ads and require digital platforms to take steps to prevent foreign entities from purchasing ads to influence US elections. This bill, however, introduces no measures to prevent domestic political operatives – including dark money groups – from using the DIM for manipulative tactics described in Part 3 of this report. "The Honest Ads Act," U.S. Senator Mark R. Warner, accessed August 8, 2018, https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act?page=1.

144 David Shepardson, "Trump Signs Repeal of U.S. Broadband Privacy Rules," *Reuters*, April 3, 2017, https://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR.

145 Emily Stewart, "The Government is Making it Easier for 'Dark Money' Donors to Go Unnamed," *Vox*, July 17, 2018, https://www.vox.com/policy-and-politics/2018/7/17/17581384/irs-dark-money-nra-maria-butina-donors.

146 The Brennen Center for Justice offers an incisive guide to well-crafted and fair legislation that could guide such legislation and ensure important exceptions for small or vulnerable donors. See: "Components of an Effect Disclosure Law" (Brennan Center for Justice, n.d.), https://www.brennancenter.org/sites/default/files/legislation/Disclosure.%20Brennan%20Center%20MiP%20Toolkit.pdf.

independent public journalism trust that could help counterbalance the drastic cuts news organization have suffered as advertising revenues shifted toward platforms.[147] All of these possibilities would require significant political will and organized advocacy efforts.

Media reform movements usually favor government regulations because, as several researchers argue, media industry self-regulation schemes often skew toward protecting businesses from criticism rather than protecting the public. [148] Nonetheless, major tech companies such as Facebook, Google, and Twitter have already taken some steps toward curtailing certain types of political manipulation through ad tech. These efforts include attempts to verify the names of a sponsoring organization or person for certain types of political ads, requiring these names to appear on ads, and creating searchable archives of such ads.[149] Still, these actions alone will not be enough to prevent many of the manipulative strategies outlined in this report. Furthermore, as Hamsini Sridharan and Ann M. Ravel note in a report for nonprofit MapLight, such steps are inconsistent across platforms and subject to change at the unilateral prerogative of executive decisions.[150] Google's US political ad policy, for instance, is narrower than Facebook's or Twitter's. Google's policy does not state that it requires sponsor verification of political issue ads but only for "election ads" that "feature a federal candidate or current elected federal officeholder in the United States."[151]

Media activists, civil society organizations, and concerned tech workers may be able to push digital advertising companies to go further to prevent DIM weaponization, even if it means revenue sacrifices. One route toward ensurin g teeth in self-regulatory promises would be to pressure companies to explicate specific steps to preventing political manipulation in user contracts and face the risk of class-action civil suits if they fail. Companies could negotiate with legal advisors working for public interest organizations, like MapLight, Common Cause, Brennen Center for Justice, and the Center for Responsive Politics, to find fair and tough language for self-regulation.

One significant further step companies could take would be to **categorically refuse to work with dark money groups**. This would mean requiring all political ad

147 Victor Pickard, "Break Facebook's Power and Renew Journalism," *The Nation*, April 18, 2018, https://www.thenation.com/article/break-facebooks-power-and-renew-journalism/.

148 Siva Vaidhyanathan, *The Googlization of Everything: (And Why We Should Worry)* (University of California Press, 2012); Angela J. Campbell, "Self-Regulation and the Media," *Federal Communications Law Journal* 51 (1999 1998): 711.

149 Sarah Perez, "Google Rolls out New Policies for U.S. Election Ads," *TechCrunch*, accessed July 7, 2018, http://social.techcrunch.com/2018/05/04/google-rolls-out-new-policies-for-u-s-election-ads/; Nellie Bowles and Sheera Frenkel, "Facebook and Twitter Plan New Ways to Regulate Political Ads," *The New York Times*, June 9, 2018, sec. Technology, https://www.nytimes.com/2018/05/24/technology/twitter-political-ad-restrictions.html.

150 Sridharan and Ravel, "Illuminating Dark Digital Politics."

151 "Political Content - Advertising Policies Help," Google, accessed September 16, 2018, https://support.google.com/adspolicy/answer/6014595?hl=en.

sponsors to publicly disclose their major donors.[152] Even when platforms require political advertisers to identify the organization sponsoring ads, such information can be of little value when it only reveals the opaque name of a dark money group. In these instances, ordinary users as well as journalists and researchers may be unable to understand the motives behind the campaign. Is a campaign being sponsored largely by a company or an industry group with financial stake in the issue? Is a campaign aimed at primarily conservative-leaning users being sponsored by Democratic donors? If they are committed to increasing ad transparency, digital advertising platforms need to ensure their users can easily find out who is behind the ads targeting them. Platforms could require LLCs, 501c(4)s, 501c(6)s, and other such groups to publicly disclose their major donors if they are going to run political ads on their services. They could also require Super PACs that receive donations from LLCs and non-profits to certify that all their donors comply with such a donor transparency policy. Such policies could pose significant costs for ad platforms. According to the Center for Responsive Politics, those political groups not disclosing any information about their donors spent over $175 million on the 2016 election cycle. Given the rising portion of ad spending that is going digital, this suggests that dark money groups will continue to spend substantial amounts on digital ads.

Reform of the DIM will also need to grapple with the prevalence of experimental testing tools in advertising systems, particularly those designed to zero in on vulnerabilities. Split testing can turn users into research subjects as campaigns probe to find just the right phrases and images that trigger emotional engagement. Such testing can be a boon to campaigns trying splinter an opponent's coalition through figuring out how to inflame internal divisions. Split testing can also help campaigns refine techniques for mobilizing one identity group by invoking threats perceived to be emanating from another. Platforms could limit this kind of weaponization by **requiring explicit, non-coercive user consent** for viewing any political ads that are part of a split-testing experiment.

Many organizations value split testing to receive feedback from their publics—often for benign purposes. To prevent users from becoming unwitting recruits in campaigns' psychological experiments, ad systems could be designed so that users need to opt in. Before viewing ad variants, users would have to agree to participate in testing experiments run by a particular sponsor. Such a design would facilitate campaigns that live up to the Marketing Research Association's Code of Standards. Through this ethics code, market researchers pledge "consent must be granted freely,

152 Implementing this rule would require deciding just how large donations would need to be to trigger the required disclosure and whether to adopt policies to consider special exemptions if organizations can make a genuine case that revealing donors would lead them to face threats and harassments—enough so to outweigh the rights of users to know who is sponsoring paid speech targeting them based on their data.

without coercion" when respondents participate in their research.[153] While an opt-in system may prove a barrier to maximizing revenue for platforms, it would help prevent their users from becoming unknowing experimental subjects.

In any case of reform, there will be trade-offs and complications. Platform companies will need guidance from a wide variety of external perspectives. Future ethical guidelines for political advertising could be developed in collaboration with **independent committees representing diverse communities and stakeholders**. Models for this kind of ethics committee include community bioethics committees at hospitals and ethics committees for artificial intelligence development.[154] Ideally, the standards created by such panels would not regulate ordinary platform users, but only the priority lanes of paid and data-enhanced speech through advertising.

Whatever the future of online ad regulation, the consideration of political ads will only be one component in a larger effort to combat disinformation and manipulation. In this report, we have described the development, features, and purpose of the Digital Influence Machine. Platform companies have invested in a vast infrastructure able to collect, process, and communicate information at an enormous scale and speed and for the purpose of leveraging powerful influence. These systems – and the algorithms underlying them – are ***invisible to users***, operating behind the scenes to hoard the data of every query, click, and keystroke. Without values like fairness, justice, and human dignity guiding the development of these technologies and a commitment to transparency and accountability underlying the deployment, such systems are antithetical to the principles of democracy.

153 Market Research Association, Code of Marketing Research Standards (adopted October 2013) https://www.insightsassociation.org/sites/default/files/misc_files/mra_code.pdf.

154 Models for this kind of ethics committee include community bioethics committees at hospitals and ethics committees for artificial intelligence development. See: Mark P. Aulisio, "Why Did Hospital Ethics Committees Emerge in the US?," *AMA Journal of Ethics* 18, no. 5 (May 1, 2016): 546, https://doi.org/10.1001/journalofethics.2016.18.5.mhst1-1605; Alex Hern, "DeepMind Announces Ethics Group to Focus on Problems of AI," *The Guardian*, October 4, 2017, sec. Technology, http://www.theguardian.com/technology/2017/oct/04/google-deepmind-ai-artificial-intelligence-ethics-group-problems.

ACKNOWLEDGMENTS

The authors would like to thank everyone who helped us develop this analysis and worked with us through many stages of refining it. Among those who generously offered us their insights or feedback on drafts are David Karpf, Matt Wood, Sandy Parakilas, Hamsini Sridharan, Ann M. Ravel, Alleen Brown, Daniel Kress, Young Mie Kim, David Vance, danah boyd, Janet Haven, Alice Leppert, Brian Creech, A.J. Bauer, Lauren Hanson, Edward Lamoureux, and Jonathan Albright. Rati Bishnoi and the communications team offered keen eyes and creative design. We're grateful for all the support of Data & Society and the Media Manipulation Team. Anthony would like to thank Ursinus College students from his Spring 2018 "Fake News and Propaganda" course who offered provocative questions, stories of their encounters with digital political ads, and reactions to early drafts. Most crucially, we want to thank our tireless and incisive editor Patrick Davison who steered us through many bloated paragraphs and tangled trails of thought.

DATA & SOCIETY

Data & Society is an independent nonprofit research institute that advances new frames for understanding the implications of data-centric and automated technology. We conduct research and build the field of actors to ensure that knowledge guides debate, decision-making, and technical choices.

www.datasociety.net
@datasociety

Design by C Studio
Illustrations by Jim Cooke