DIGITAL MARKETING IN THE DISINFORMATION AGE

Douglas Guilbeault

Abstract: Major social-media companies profess liberal values like global community and democratic participation as primary incentives motivating the design of their platforms and their proposed solutions to online disinformation. However, the industry of digital marketing that underlies these companies' business models is in tension with these values. Digital marketing ascribes more value to users from demographics with higher socioeconomic status, and online disinformation campaigns that harness the infrastructure of digital advertising built into social media undermine democratic participation. Regulators and the public have called on social-media companies to address the global rise of online disinformation, emphasizing the detection and removal of foreign actors, particularly Russian hackers. This essay argues that the contentious narrative of foreign actors in online disinformation distracts from the foundational role of digital marketing in driving the spread of disinformation online with implications for the design of effective regulation.

The 21st century became known as The Information Age due to the hope that global communication technologies would spur the spread of liberal democracy and usher in an era of unprecedented cooperation among nations.[1] This vision underlies Facebook founder and CEO Mark Zuckerberg's manifesto, "Building Global Community," in which he tasks his creation with the goals of alleviating poverty, ending terrorism, fighting climate change, preventing pandemics, and spreading democracy around the world. Evan Williams, co-founder of Twitter, has expressed similar aspirations.[2] However, the rise of computational propaganda has marred social media by clouding public discourse, fragmenting audiences, and inciting cyberwar. Perhaps the 21st century should be more aptly named The Disinformation Age.

In response to Russian interference in the 2016 U.S. election, social-media platforms touted liberal ideals in their effort to prevent foreign influence. As

Zuckerberg expressed in his prepared statement to congress:

> Facebook's mission is about giving people a voice and bringing people closer together. Those are deeply democratic values and we're proud of them … Advertisers and developers will never take top priority over that as long as I'm running Facebook.[3]

In his testimony on Russian interference, Zuckerberg repeatedly distanced himself from advertisers. According to Zuckerberg, "bad actors" were able to hack Facebook's system by taking advantage of their advertising tools to disseminate malicious propaganda.[4] While Zuckerberg's testimony highlighted digital marketing as a contributor to online disinformation, it also created the false impression that digital marketing drives disinformation only if vulnerable to manipulation. But as this essay argues, digital marketing actually drives online disinformation. With digital ad revenues as their primary source of profit, social-media companies have designed their platforms to influence users on behalf of marketers and politicians, both foreign and domestic. These practices are fundamentally at odds with the liberal values the companies profess.

Social-media companies face a paradox of incentives. Underlying the goal of fostering global community are the ideals of liberalism, where all people are treated equal and are empowered to participate in a marketplace of ideas. Yet in the logic of digital marketing, certain demographics are more valuable than others. Digital marketing appeals to users who have the money and time to spend on products online. This dynamic can be observed in Facebook's advertising revenue report.

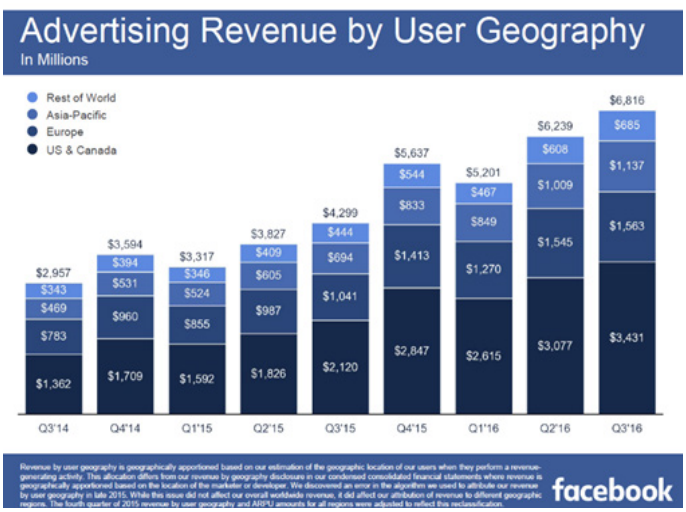

Figure 1: Facebook's quarterly advertising revenue broken down by geographical region. This image is copied from the public slides that Facebook used to present its quarterly reports. More information on these numbers can be found in Facebook's Securities and Exchange Commission, Form 10-Q, Washington D.C. 20259 (2017).

Figure 1 displays Facebook's quarterly advertising revenue from 2014 to 2016 categorized by geography. The vast majority of this revenue comes from users in the United States and Canada, which together generate over twice as much revenue as Europe, the second-largest source of Facebook's revenue. This is despite the fact that India now has the largest number of Facebook users. The remaining countries in the top-five—Brazil, Indonesia, and Mexico—constitute a much larger user base. Yet only the US and Canada are explicitly named as primary national markets, while countries with millions of users are homogeneously categorized as the "rest of the world."[5,6]

Digital marketing directly shapes the design of social-media interfaces. Careful scholarship shows how various interface features, such as Facebook's timeline or Twitter's trending algorithm, nudge users to share more of their personal data.[7,8,9] Indeed, Sean Parker, ex-president of Facebook, admitted that Facebook designed its interface with the intention of making the platform addictive to maximize the extraction of lucrative data from users.[10] According to Parker, the makers of Facebook predicted that public displays of social capital, such as numbers of friends and likes, would hijack neural reward systems to increase habitual dependence. A leaked Facebook memo, corroborating Parker's testimony, outlined statements from Andrew Bosworth, a Facebook executive, who defended the company's use of digital advertising as an "ugly growth tactic" even if it meant that people could use their platform to inflict great harm.[11]

Digital marketing translates directly into incentives for eliciting personal data because; (1) platforms can sell this data to third parties and; (2) they can use data to refine their micro-targeting algorithms, which are among their most valuable products.[12] Social-media companies use personal data to construct predictive models of user behavior, and advertisers bid over these models in massive markets.[13,14] With these models, Facebook can monitor users' posts and photos in real time.[15] Such massive datasets are invaluable to advertising agencies, which regularly exploit anxiety and self-esteem to market products.[16] Because the incentives of marketers can lead to exploitation, the US passed the Children's Television Act (Pub. L. 101-437) and the Children's Online Privacy Protection Act (Pub. L. 105-277) to regulate media content for children. However, social-media companies are not subject to these regulations, because under the Communications Decency Act (CDA 230), social media companies define themselves as neutral distributors of user-generated content, without playing an active role in editing or endorsing this content.[17,18]

Hacking Platform Design for Disinformation

Narrowly focusing on foreign interference as the source of disinformation is

a mistake. There is a problematic emphasis on the ingenuity of Russian hackers, as if their election interference was solely due to technical capabilities. In reality, their tactics used the influence infrastructure already available on social media.[19] As a recent study on the digital-advertising industry reported: "Russia's Election Interference is Digital Marketing 101."[20,21] The study shows how Russian interference in the 2016 election made extensive use of Facebook's tools for microtargeting and advertisement distribution. Facebook's micro-targeting services enhanced these campaigns by allowing marketers to target based on ethnicity, sexual orientation, political affiliation, and controversial categories such as "Jew hater."[22] If there is any ingenuity to ascribe to those who interfered on behalf of Russia, it would be in their realization that their target had already designed weapons of mass influence that could be used against them.

Domestic actors can also exploit the influence mechanisms built into social media technologies. One case in point is Cambridge Analytica. In his congressional testimony, Zuckerberg explained how in 2013, Aleksandr Kogan at Cambridge University created a personality quiz application that gained access to the private data of tens of millions of users, due to Facebook's data policies at the time.[23] Even though Facebook revised its policies in 2014, this did not prevent Kogan from sharing the data with Cambridge Analytica, which then deployed an arsenal of disinformation tactics to support the presidential campaign of then-candidate Donald Trump.[24]

Effects of Digital Advertising on the Bot Economy

The mainstream discussion of Russian interference has concentrated on one technology in particular: the bot. The popular narrative portrays bots as sophisticated technologies of mass manipulation deployed by Russian hackers and other bad actors. This is flawed for two reasons. First, bots are not a technology devised uniquely for foreign interference; in fact, the earliest evidence of bot influence was traced to a race in Massachusetts in 2010.[25,26] Second, bots are not sophisticated. They often involve simple scripts that amateur programmers can implement.[27] The ability of bots to influence humans depends on how they exploit the interface features and communicative tools.[28] For those who cannot code, bots can be purchased for nearly every platform in active online marketplaces. Facebook claims it has nearly eliminated bots from its platform using two-factor authentication, but many fake accounts have been operated by individuals for years, and so are fully authenticated and indistinguishable from real users.

The same group of people who supply social-media platforms with their advertising revenue is contributing to the growth of a technology used to wage disinformation campaigns. Both Twitter and Facebook have dragged their feet on devel-

oping regulations against bots, most likely due to conflicting incentives.[29] Both Twitter and Facebook stand to benefit financially from bots and bot-driven traffic, which stir user activity and circulate attention-grabbing content. Additionally, Facebook has invested millions of dollars into bot-based applications that can be used for customer service and disseminating digital advertisements.[30,31] Meanwhile, Facebook and other major technology companies like IBM are investing in the design of AI-powered bots, capable of both socializing with users and generating predictive models of their behavior.[32]

The Role of Regulation

At present, social media companies are responsible for addressing disinformation and bots. In his congressional testimony, Zuckerberg outlined a number of internal regulations that Facebook is implementing. For example, Facebook now requires all political advertisements to be associated with Facebook pages describing their funders and advertising history. Zuckerberg and other social media leaders have expressed support for the Honest Ads Act, a bill aimed at extending regulations for political advertising on television and radio to social media.[33] If passed, the Honest Ads Act would require all political advertising on major social-media companies to disclose the identity of their funder, as well as information about their target audience and money spent on the campaign. The Honest Ads Act would also increase the strength of regulations protecting against foreign investment in domestic electioneering.

While the move toward federal regulation holds promise, current efforts will still leave many issues to internal regulation, providing leeway for companies to safeguard their interests. Facebook has developed a plan to control fake news by downvoting suspicious content. These regulations are led by Katie Harbath, a former Republican digital strategist and current director of Facebook's global government and politics team. Harbath's philosophy taps into what Ferguson calls the "False Prophecy" of social media, which is the belief that by increasing the size and activity of online social networks, a collective intelligence effect will emerge that will filter out the truthful content from the fake and malicious content.[34] Twitter co-founder Evan Williams has expressed similar hopes: "I thought once everyone could speak freely and exchange information and ideas, the world is automatically going to be a better place."[35]

In fact, Facebook directly embeds employees in political campaigns around the world.[36] In the US, the unit embedded employees in Trump's campaign; the Clinton campaign denied the request. In India, the company built the online reputation of Prime Minister Narendra Modi, who has more Facebook followers than any other leader in the world. In the Philippines, this team trained the campaign

of Rodrigo Duterte. And in Germany, it helped the anti-immigrant Alternative for Germany Party (AfD) win its first Bundestag seat. Investigative journalists argue: "Politicians running for office can be lucrative ad buyers". Here the paradox of incentives becomes clear: the same team tasked with defending against disinformation is also training political actors on how to use their platform for propaganda.

In *How Propaganda Works*, philosopher Jason Stanley explains that a common technique is for an organization to profess a philosophy that, in practice, is the opposite of its political actions.[37] This strategy is most effective, Stanley maintains, when the hypocrisy is not apparent even to the propagandist. The liberal philosophy of social-media platforms recreates this pattern. Hwang[38] suggests that social-media companies have incentives to sustain, and even encourage, the spread of fake news on their platform because click-bait and inflammatory content circulates much faster and for much longer, thereby increasing user activity.[39] At present, the public is limited in its ability to determine whether Facebook's policy decisions are motivated by liberal ideals or corporate interests.

Conclusion

The solution to disinformation will require a delicate balance of external and internal regulation. Some of the greatest challenges concern how the technologies and actors involved are defined in the legal context.[40] The Honest Ads Act contains crucial ambiguities that may undermine it. For instance, the authors designed the bill to apply only to social-media companies with more than 50 million U.S. visitors every month. However, a common disinformation tactic employed during the 2016 U.S. election involved the use of advertisements and fake user content to lure people onto small blogging websites and discussion forums where they were exposed to more extreme content.[41] Under the Honest Ads Act, media content on smaller, more niche websites would fall outside the scope of regulation even though they are equally a part of the media ecosystem. This is demonstrated by a recent case where a fake news story produced by trolls on 4chan was shared by Google News and subsequently linked via Facebook's crisis response page.[42]

Researchers have called into question the extent to which the Honest Ads Act can be applied to major social-media companies, given that social-media companies have yet to be categorized as media providers under key regulations like Section 230 of the Communications Decency Act. Any narrative that draws attention away from the systemic effects of digital marketing on disinformation is likely to lead to misunderstandings of social-media technology and the development of inadequate policies to regulate it.♔

Douglas Guilbeault *is a Ph.D. Candidate in the Annenberg School for Communication at*

the University of Pennsylvania. He is a member of the Network Dynamics Group (NDG), where he uses online experiments to study the effects of network structure on collective intelligence and political communication. Douglas is also a member of the Computational Propaganda Project at the Oxford Internet Institute, where he focuses on the technical and political implications of disinformation technology, particularly political bots. His journalism on bots has appeared in the Atlantic, Wired, and Quartz; his academic articles have appeared in the Proceedings of the National Academy of the Sciences, Policy & Internet, the International Journal of Communication, and the Journal of Cognitive Linguistics. His research is funded by the Social Sciences and Humanities Research Council of Canada and the Institute for Research on Innovation and Science at the University of Michigan. He is also a member of the DigIntel lab at the Institute for the Future.

NOTES

1 James Gleick, *The information: A history, a theory, a flood* (New York, NY: Pantheon Books, 2011).

2 David Streitfeld, "The Internet Is Broken": @ev Is Trying to Salvage It," *The New York Times*, 20 May 2017, https://www.nytimes.com/2017/05/20/technology/evan-williamsmedium-twitter-internet.html.

3 Emily Stewart, "Read: Mark Zuckerberg's Prepared Statement for Congressional Testimony," *Vox*, 10 April 2018, https://www.vox.com/policy-and-politics/2018/4/9/17215640/mark-zuckerberg-congress-testimony-facebook.

4 Ibid.

5 Sandra González-Bailón, "Social Science in the Era of Big Data," *Policy and Internet* 5, no. 2 (2013), 147–60.

6 Gina Neff and Dawn Nafus, *Self-tracking* (Cambridge, MA: MIT Press, 2016).

7 Zizi Papacharissi, "The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn, and ASmallWorld," *New Media & Society* 11, nos 1–2 (2016), 199–220.

8 Jose Van Dijck, "'You have one identity': Performing the self on Facebook and LinkedIn," *Media, Culture & Society* 35, no. 2 (2013), 199–215.

9 Alice Marwick, *Status Update: Celebrity, Publicity, and Branding in the Social Media Age* (New Haven, NJ: Yale University Press, 2015).

10 Julia Glum, "Facebook is Addictive Because it 'Exploits a Vulnerability' in People's Brains, Co-founder Sean Parker Says," *U.S. News Week*, 10 November 2017, http://www.newsweek.com/russia-facebook-trump-sean-parker-707964.

11 Jillian D'Onfro, "Facebook exec in 2016 internal memo defends 'ugly' growth tactics, even if people use platform for evil," *NBC News: Tech*, 29 March 2018, https://www.cnbc.com/2018/03/29/facebook-exec-andrew-bosworth-2016-ugly-memo-growth-at-all-costs.html.

12 Antonio Martinez, *Chaos Monkeys: Obscene Fortune and Random Failure in Silicon Valley*, (New York: Harper, 2016).

13 Joseph Turow, *The Daily You*, (New Haven, CT: Yale University Press, 2011).

14 Joseph Turow, *The Ailes have Eyes: How Retailers Track your Shopping, Strip your Privacy, and Define your Power*, (New Haven, CT: Yale University Press, 2017).

15 Darren Davidson, "Facebook targets 'insecure' young people," *The Australian*, 1 May 2017, http://www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

16 Joel Bakan, *Childhood Under Siege: How Big Business Targets Children*, (New York: Free Press, 2011).

[17] Paul Ehrlich, "Communications Decency Act 230," *Berkeley Technology Law Journal* 17, no. 1 (2002), 401–419.

[18] Tim Hwang, *Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment* (2017).

[19] Alexis Madrigal, "Russia's Troll Operation was not that Sophisticated," *The Atlantic*, 19 February 2018, https://www.theatlantic.com/technology/archive/2018/02/the-russian-conspiracy-to-commit-audience-development/553685/.

[20] Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," *New America: Public Interest Technology* (2018), https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

[21] Dipayan Ghosh and Ben Scott "Russia's Election Interference is Digital Marketing 101," *The Atlantic*, 19 February 2018, https://www.theatlantic.com/international/archive/2018/02/russia-trump-election-facebook-twitter-advertising/553676/.

[22] Julia Angwin, Madeleine Varner, and Ariana Tobin, "Facebook Enabled Advertisers to Reach 'Jew Haters,'" *ProPublica*, 14 September 2017, https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

[23] Stewart (2018).

[24] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fall Out so far," *The New York Times*, 4 April 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[25] Panagiotis T. Metaxas and Eni Mustafaraj, "Social Media and the Elections," *Science* 338, no. 6106 (2012), 472–473.

[26] Douglas Guilbeault and Samuel C. Woolley, "How Twitter Bots are Shaping the Election," *The Atlantic*, 1 November 2016, http://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/.

[27] Samuel C. Woolley and Philip N. Howard, "Political Communication, Computational Propaganda, and Autonomous Agents: Introduction," *International Journal of Communication* 10 (2016), 4882–90.

[28] Douglas Guilbeault, "Growing Bot Security: An Ecological View of Bot Agency," *The International Journal of Communication* 10 (2016), 5003–21.

[29] Robert Gorwa and Douglas Guilbeault, "Unpacking the Social Media Bot: A Typology to Guide Research and Policy," *Policy & Internet* 10, no. 2 (2018), https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.184.

[30] Josh Constine, "Facebook Messenger launches group bots and bot discovery tab," *Tech Crunch*, 18 April 2017, https://techcrunch.com/2017/04/18/facebook-bot-discovery/.

[31] Alex Tarrand, "Facebook Messenger Bots: What Every Marketer Needs to Know," *Adweek*, 29 December 2017, http://www.adweek.com/digital/alex-tarrand-lucktastic-guest-post-facebook-messenger-bots/.

[32] Douglas Guilbeault and Joel Finkelstein, "Human-bot Ecologies," Z. Papacharissi, ed, *A Networked Self: Human Augmentics, Artificial Intelligence, Sentience* (Routledge, 2018).

[33] Civic Impulse, S.1989–115th Congress: Honest Ads Act (2018), https://www.govtrack.us/congress/bills/115/s1989.

[34] Niall Ferguson, "The False Prophecy of Hyperconnection," *Foreign Affairs* 96, no. 5 (2017), 68–79, https://www.foreignaffairs.com/articles/2017-08-15/false-prophecy-hyperconnection.

[35] David Streitfeld (2017).

[36] Lauren Etter, Vernon Silver, and Sarah Frier, "How Facebook's Political Unit Enables the Dark Art of Digital Propaganda," *Bloomberg Technology*, 21 December 2017, https://www.bloomberg.com/news/features/2017-12-21/inside-the-facebook-team-helping-regimes-that-reach-out-and-crack-down.

[37] Jason Stanley, *How Propaganda Works* (Princeton, NJ: Princeton University Press, 2016).

[38] Tim Hwang, "Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment," *SSRN Research Journal* (2017).

[39] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science*

359, no. 6380 (2018), 1146–51, https://doi.org/10.1126/science.aap9559.

[40] Robert Gorwa and Douglas Guilbeault (2018).

[41] Alica Marwick and Rebecca Lewis, "Media Manipulation and Disinformation Online," *Data and Society Research Institute Report* (2017).

[42] Sam Machovech, "Google admits citing 4chan to spread fake Vegas shooter news," *Arstechnica*, 2 October 2017, https://arstechnica.com/information-technology/2017/10/google-admits-citing-4chan-to-spread-fake-vegas-shooter-news/.