Diminishing Russian Influence: Overcoming Coordinated Disinformation Operations through Federal Policy

Dipayan Ghosh

January 23, 2020

DAY ONE PROJECT

dayoneproject.org

Summary

Internet-based disinformation operations have infiltrated the universe of political communications in the United States. American politics and elections carry major implications for the national and global economy as well as for diplomatic relations conducted by and with the United States. As a result, the United States is a major target for politically charged propaganda promulgated by both foreign and domestic actors. The 2016 presidential election is a case in point. Although the overall impact of Russian disinformation operations in the 2016 election has not been conclusively determined, many have suggested that such operations swung thousands of votes in key swing states, possibly affecting the final election outcome.[1] Further, the threat presented by the disinformation problem appears to only be growing as more and more technological pathways for its spread continue to develop and increasing numbers of bad actors come to learn of the opportunities inherent in disseminating coordinated political falsehoods.[2]

The federal government should pursue a two-part approach to countering internet-based disinformation. The first part should target disinformation operations here and now. Through a combination of executive actions, Congressional engagement, and collaboration with leading internet platforms, the president can position the federal government to contain and dismantle disinformation operations as they are identified. Achieving this goal, and enabling the United States to protect national elections in real time, will require actions such as:

- Designing structured opportunities for engagement and coordination between the industry and government.
- Developing information-sharing programs to facilitate collaboration in identifying and stunting disinformation operations.
- Establishing clear regulations regarding what content and operations should be removed from internet platforms.
- Encouraging advancements in artificial intelligence that can guard against disinformation.

The second part presents an even greater challenge: to establish a comprehensive regulatory regime for internet companies that protects the public from the disinformation problem in perpetuity. Achieving this goal requires the next administration to first acknowledge the direct link between disinformation and commercial internet business

[1] Jane Mayer, "How Russia Helped Swing The Election For Trump", The New Yorker, September 24, 2018. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.

[2] Alexandra Levine et al, "Why The Fight Against Disinformation, Sham Accounts And Trolls Won't Be Any Easier In 2020", Politico, December 1, 2019, https://www.politico.com/news/2019/12/01/fight-against-disinformation-2020-election-074422.

models, and then to regulate those business models intelligently such that overreaches are contained.

1. Challenge and opportunity

Three factors have contributed to the rise of political disinformation in the United States. These are:

(1) The creation, cultivation, and expansion of compelling internet-based platforms (e.g., Apple News Feed, Facebook Messenger, Instagram, Amazon, Google Search, and YouTube) that are algorithmically designed to maximize user engagement, alongside anticompetitive acts by platform owners to suppress market rivals.[3]

(2) The uninhibited collection of individual personal information (often without user awareness) through such platform services. This enables platform owners to develop and maintain detailed behavioral profiles on individual users and then apply those profiles to serve engaging content, including targeted advertising.

(3) The development and ongoing refinement of highly opaque and increasingly intricate artificial intelligence systems designed to curate social feeds and target advertisements at individual users.[4]

Current U.S. regulations place few—if any—meaningful restrictions on these activities. The combination of high user engagement with online platforms and limited federal oversight of such platforms has created an environment ripe for sophisticated, internet-based political communication campaigns. Legitimate and illegitimate operators alike can easily leverage user data to craft political messages targeted at specific audience segments and deliver messages in ways that make it very difficult for individuals to gauge their integrity. The problem is exacerbated by the corrosive business model that underlies many internet platforms—a model that derives commercial value from the spread of *any* content, whether harmful or not.

"Tracking-and-targeting" ad-delivery systems have subverted the U.S. democratic process. Our democracy is premised on the assumption that citizens can and will judge political issues and leaders on their factual merits. But this assumption is invalidated

---

[3] *See, e.g.*, European Commission, "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising", March 20, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770; Hannah Kuchler, "Facebook accused of 'anti-competitive' behavior" *Financial Times*, May 24, 2018, https://www.ft.com/content/a383ab46-5f6b-11e8-9334-2218e7146b04; European Commission, "Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon", July 17, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291.

[4] Dipayan Ghosh, "A New Social Contract to Encourage Internet Competition", Antitrust Chronicle, Competition Policy International, April 17, 2019, https://www.competitionpolicyinternational.com/a-new-digital-social-contract-to-encourage-internet-competition/.

when (1) most citizens get most of their political information through internet-based platforms, and (2) the spread of political *disinformation* aligns with the commercial interests of internet-based platforms.

Although political bias has always pervaded the media landscape, the nature and magnitude of today's disinformation problem is unprecedented. Traditional media such as broadcast television and radio are protected against disinformation campaigns due to stringent governmental regulations and top-down control of media outlets. By contrast, digital media are relatively unregulated, open-access, and decentralized. Foreign disinformation operators can easily leverage digital ad networks to push manipulative content—including political conspiracies and falsehoods—at segments of the voting population they deem vulnerable to it. This insidious form of election interference is both highly effective and difficult to detect.

Some internet-based platforms, such as Facebook and Google, have recently taken steps to limit political targeting and the spread of disinformation.[5–7] Platform operators have changed how content is curated, partnered with news organizations for fact-checking, and strengthened cybersecurity against foreign interference. But—as illustrated by recent disinformation incidents in the United States[8], Britain,[9] and Sweden[10]—these steps have not gone far enough. The problem is one of both will and capacity. It is difficult to imagine platform operators taking adequate voluntary actions to contain the disinformation problem when it is not in their commercial interest to do so. Tracking-and-targeting ad-delivery systems generate enormous profits for internet-based platforms whether used by legitimate or illegitimate operators. Hence voluntary restrictions imposed by platform operators on these systems are more likely to be surface-level concessions to public outcry rather than earnest attempts to curb the spread of disinformation. And even if a subset of platform operators are truly motivated to address the disinformation problem, they will find it impossible to do so alone. Federal oversight is needed to safeguard against disinformation campaigns and foreign interference throughout the entire digital-media landscape.

2. Proposed action

[5] Patience Haggin, "Google to Restrict Political Ad Targeting on Its Platforms", *The Wall Street Journal*, November 20, 2019, https://www.wsj.com/articles/google-to-restrict-political-ad-targeting-on-its-platforms-11574293253.
[6] Emily Glazer, "Facebook Weighs Steps to Curb Narrowly Targeted Political Ads", *The Wall Street Journal*, November 21, 2019, https://www.wsj.com/articles/facebook-discussing-potential-changes-to-political-ad-policy-11574352887.
[7] Dipayan Ghosh, "Banning Micro-Targeted Political Ads Won't End the Practice", *WIRED*, November 22, 2019, https://www.wired.com/story/banning-micro-targeted-political-ads-wont-end-the-practice/.
[8] Davey Alba, "Facebook Bans Ads", *The New York Times*, August 23, 2019, https://www.nytimes.com/2019/08/23/technology/facebook-ads-epoch-times.html.
[9] Ben Nimmo, *UK Trade Leaks*, Graphika (December 2019).
[10] Chloe Colliver, *et al.*, *Smearing Sweden: International Influence Campaigns in the 2018 Swedish Election*, ISD (November 2018).

The next administration should pursue a two-part strategy to combat the spread of disinformation through internet-based platforms. This strategy should focus on (1) identifying and neutralizing acute, near-term disinformation threats, and (2) realigning economic incentives in order to mitigate the disinformation problem in perpetuity.

2.1 Addressing disinformation in the near term

Many near-term disinformation threats can be contained as they arise. The apparently minimal effects of foreign disinformation operations in the 2018 U.S. midterm elections is largely attributable to the success of counter-disinformation practices implemented by internet-based platforms in coordination with the federal government.[11] The federal government can and should continue to work with industry partners to identify and neutralize acute, near-term disinformation threats, including through the actions outlined below.

Establish a clear framework for industry-governmental engagement around disinformation

The intelligence community needs a clear understanding of how leading internet-based platforms plan to contain disinformation in the lead-up to every major election – and correspondingly, internet platforms can benefit from the intelligence agencies' capacities in information-sharing and analysis. The federal government should ensure that representatives of relevant federal agencies and key industry partners meet frequently to coordinate counter-disinformation operations. So that all concerns emerging from the industry have the opportunity to be raised, meetings should be conducted on both an industry-wide basis and on an individual-firm basis. We caution that while an administration can play a vital role in fostering industry-governmental relations, deference should be given to civil-service members of the intelligence community when determining the specifics of industry-governmental partnerships.

Advance an information-sharing agreement among internet-based platform operators

The intelligence community, in partnership with the National Security Council, should advance an information-sharing agreement among internet-based platform operators designed to combat the spread of disinformation. Under such an agreement, any member operator that detected a disinformation effort would have the opportunity (or obligation) to report the nefarious activity to the group of firms. Such an agreement could

[11] Daniel Funke, "There was less misinformation during the midterms than 2016. But its form has changed", The Poynter Institute, https://www.poynter.org/fact-checking/2018/there-was-less-misinformation-during-the-midterms-than-in-2016-but-its-form-has-changed/.

mirror the structure of cybersecurity information-sharing programs that have already been established by industry and the intelligence community.

Where possible, establish standards for intolerable content

There is much debate over where the line for removing content should be drawn. The desire to remove content that triggers hate, revulsion, or violence inevitable conflicts with the desire to protect free-speech rights afforded by the First Amendment. The federal government should work with industry to establish standards for intolerable content and methods for implementation, including in the contexts of disinformation, hate speech, harassment, and incitement to radicalization, violence, and/or terrorism. Some companies are already beginning to establish such standards when it comes to disinformation. Facebook, for instance, has announced that it will unilaterally take down content it can identify as having originated from the Internet Research Agency.[12] In addition to considering who originated content, disinformation standards may also consider factors such as who disseminated the content, where it originated from, who paid for it, whether the content was political in nature, and what messages the content contained.

Support advancements in artificial intelligence to efficiently counter disinformation

The leading internet-based platforms have achieved tremendous scale. Facebook exceeded two billion users in 2017[13]; Gmail passed 1.5 billion in 2019[14]; and YouTube passed 1.9 billion in 2019.[15] The content generated by such large userships is vast and difficult to monitor in real time.[16] Advancements in artificial intelligence (AI) are needed to ensure that disinformation can be detected and suppressed before reaching large audiences. The next administration should work with platform operators to review existing AI systems available to combat disinformation and identify shortcomings. The administration should then incentivize platform operators, researchers, and startups to address these gaps. Options include increasing federal funding for research related to counter-disinformation AI, conducting "hackathons" and prize competitions designed to elicit innovative solutions in a short period of time, and establishing corporate exchange

[12] Alex Stamos, "Authenticity Matters: The IRA Has No Place On Facebook", Facebook, April 3, 2018, https://about.fb.com/news/2018/04/authenticity-matters/.
[13] Kaya Yurieff, "Facebook Hits 2 Billion Monthly Users", CNN, June 27, 2017, https://money.cnn.com/2017/06/27/technology/facebook-2-billion-users/index.html.
[14] Jennifer Elias and Magdalena Petrova, "Google's Rocky Path To Email Domination", CNBC, October 26, 2019, https://www.cnbc.com/2019/10/26/gmail-dominates-consumer-email-with-1point5-billion-users.html
[15] Maryam Mohsin, "10 Youtube Stats Every Marketer Should Know in 2020", Oberlo, November 11, 2019, https://www.oberlo.com/blog/youtube-statistics.
[16] Tarleton Gillespie, "The Scale Is Just Unfathomable", Logic Magazine #4, April 1, 2018, https://logicmag.io/scale/the-scale-is-just-unfathomable/.

programs whereby members of the private sector can learn from the government intelligence community and vice versa.

2.2 Impose regulations to mitigate disinformation in perpetuity

As explained in Section 1, there is a direct link between the profit incentives of internet-based platforms and the prevalence of disinformation today. Severing this link will require the federal government to impose regulations that (1) advance market competition in the internet industry, (2) improve consumer privacy standards, and (3) promote transparency surrounding the complex algorithms widely used in the internet industry. Specific policy recommendations for each of these areas follow.

Competition

Market concentration in the consumer internet industry is rapidly increasing. Facebook dominates U.S. markets for social media and internet-based text messaging; Google dominates markets for internet search, email, and online video; and Amazon dominates e-commerce. Monopoly status in and of itself traditionally does not trigger regulatory scrutiny in the United States. Moreover, the United States has in recent decades adopted a light-touch approach to competition enforcement—with judgements dependent on the demonstration of explicit consumer harm.

Experts argue that this regulatory regime has allowed "big tech" companies to operate at the expense of the American public. Because internet-based platforms generate value in ways that are not directly connected to the prices or quality of goods and services, the monopoly powers of these platforms do not always cause "explicit consumer harm" in the traditional sense. Yet the rise of disinformation is arguably a consumer harm triggered by the unchecked rise of a few dominant platforms.

Under the Trump Administration, the Justice Department and Federal Trade Commission (FTC) have already initiated some investigations of the consumer internet industry.[17] But it remains unclear where these inquiries will lead and how—if at all—they will affect the monopoly behavior of big tech companies. There are several actions the next administration can take to further promote competition in consumer internet. One action is to direct the FTC to reassess its 2015 Statement of Enforcement Principles Regarding "Unfair Methods of Competition." Another is to consider developing or endorsing legislation that would expand the capacity and jurisdiction of federal

[17] Daisuke Wakabayashi, Katie Benner, and Steve Lohr, "Justice Department Opens Antitrust Review of Big Tech Companies", *The New York Times*, July 23, 2019, https://www.nytimes.com/2019/07/23/technology/justice-department-tech-antitrust.html.

authorities (including antitrust authorities) on inquiries related to market concentration and consumer exploitation in the internet industry.

Privacy

The primary economic regulation that can blunt the disinformation problem with immediate effect is meaningful privacy reform. Limiting the capacity of internet-based platforms to collect data on individual users will limit the development of individual behavioral profiles that enables microtargeting of political ads. The next administration should work with Congress on legislation similar to the European General Data Protection Regulation[18] that gives consumers a clear right to the information internet-based platforms collect on them, including control over behavioral data of the kind gathered by Aleksandr Kogan and thereafter sold to Cambridge Analytica – including raw data pertaining to location records, web browsing history, on-platform engagement history and data broker data that, in sum, is used by internet firms to compose behavioral profiles that indicate the user's likes, dislikes, preferences, beliefs and routines. This legislation should make it clear that privacy rights apply to historical data as well as data that may be collected in the future. The principal driving force behind this legislation must be that a particular user has complete control over who can store, access, and disseminate any data on that user.

Transparency

Promoting transparency in the internet industry is critical to enabling journalists, researchers, and the public to understand the extent and impact of disinformation operations. The Administration should work with Congress to require internet-based platforms to disclose several key pieces of information for all political advertising conducted on such platforms. These pieces of information are: (1) the creator of the ad campaign, (2) the entity responsible for funding the ad campaign, and (3) measures concerning the reach and viewership of the ad campaign. These data points should be directly available to platform users alongside every ad delivered—not in a database on another website. To enable in-depth research and analysis, internet-based platforms should also be required to establish and maintain databases with API features that include the aforementioned details about historical and current on- and off-platform advertising campaigns.

3. Conclusion

Disinformation operations conducted through internet-based platforms undermine the American democratic system and create a clear and present danger for members of the

[18] Intersoft Consulting, "General Data Protection Regulation: GDPR", n.d., https://gdpr-info.eu/.

American public. The time has come for meaningful new regulations that will hold big tech companies accountable for the content published on their platforms. Success will require a coordinated, whole-of-government approach spearheaded by the White House – with leadership in the Office of Science and Technology Policy, National Security Council and National Economic Council – in close coordination along with the Department of Justice, Department of Commerce, and intelligence community. The federal government should pursue a two-part strategy to combating the spread of disinformation through internet-based platforms. The first part of this strategy should focus on working the intelligence community and the consumer internet industry to tackle acute disinformation threats as they arise. The second should focus on imposing legislative reforms in transparency, privacy, and competition policy that combat internet-based disinformation campaigns in perpetuity. Throughout history the United States has favored the openness of markets, but we have not hesitated to curb their expanse the moment they implicate the foundations of our national political process. This is the juncture we have reached with the American technology industry; we must act in the interest of the citizen.

About the author

Dipayan Ghosh is Co-Director of the Digital Platforms & Democracy Project and a Shorenstein Fellow at the Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School, where he works on digital privacy, artificial intelligence, and civil rights. He is also a Lecturer on Law at Harvard Law School, where he teaches on the economics of internet monopolization. Dipayan previously worked on global privacy and public policy issues at Facebook, where he led strategic efforts to address privacy and security. Prior, Dipayan was a technology and economic policy advisor in the Obama White House. He served across the Office of Science and Technology Policy and the National Economic Council, where he worked on issues concerning big data's impact on consumer privacy and the digital economy. Dipayan has served as a Public Interest Technology fellow at New America, the Washington-based public policy think tank. He received a Ph.D. in electrical engineering & computer science at Cornell University and completed postdoctoral study in the same field at the University of California, Berkeley.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of a future presidential term. For more about the Day One Project, visit dayoneproject.org.