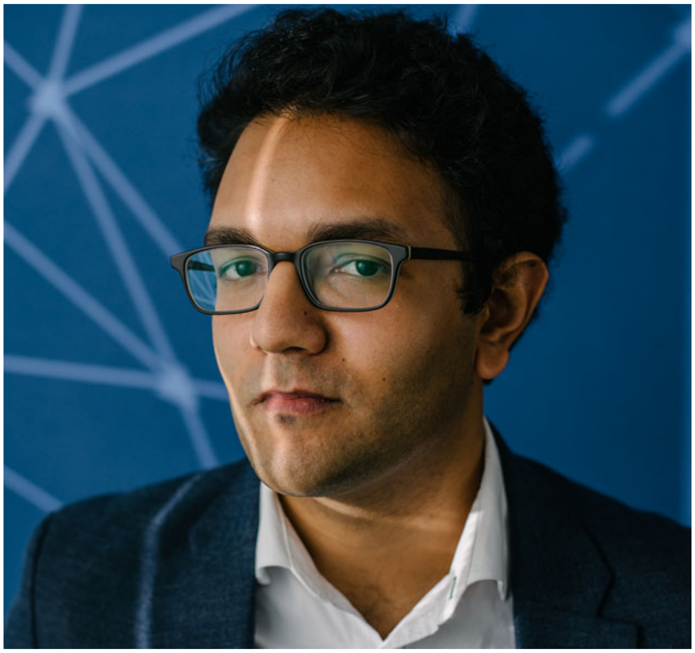
National Endowment for Democracy
Supporting freedom around the world

forum
International Forum for Democratic Studies

FORUM Q&A: DIPAYAN GHOSH ON THE COMMERCIAL DRIVERS OF PRECISION PROPAGANDA



Dipayan Ghosh is a fellow at New America and the Shorenstein Center at the Harvard Kennedy School, where he writes on the ways that modern internet technology are affecting politics, privacy, and autonomy. A computer scientist and privacy engineer by training, Ghosh was a technology and economic policy advisor in the Obama White House, where worked on many of the administration's policy initiatives concerning consumer privacy, net neutrality, cybersecurity, and spectrum policy. Most recently, Ghosh was the U.S. privacy and public policy advisor for Facebook. He left the company shortly after the 2016 presidential elections to explore the growing interactions between the world's largest internet platforms, the traditional news media, and the American political culture. Follow him on Twitter @Ghoshd7.

The spread of state-generated disinformation through social media has called technology platforms' impact on public discourse into question. While many have scrutinized social media's influence on news consumption, the commercial aspects of digital disinformation remain relatively underappreciated. Through behavioral data tracking, targeted advertising, search engine optimization, and other techniques originally developed for digital marketing, purveyors of disinformation are able to reach audiences like never before through "precision propaganda."

Dean Jackson of the International Forum for Democratic Studies spoke with Dipayan Ghosh about his report with Ben Scott for New America, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," which describes the technologies used both to sell ads to consumers and peddle disinformation to citizens. (This interview has been condensed and edited for clarity. The views and opinions expressed within do not necessarily reflect those of the National Endowment for Democracy.)

Dean Jackson: In your report, you write that "political disinformation succeeds because it follows the structural logic, benefits from the products, and perfects the strategies of the broader digital advertising market." Can you give our readers some brief examples of how this is true in practice?

Dipayan Ghosh: The Russians did absolutely nothing that is beyond any digital marketing professional who works for a company to manage its social media. Our main argument is that there is an implicit but extraordinarily powerful alignment in the goals of the global internet platform and those of the disinformation operator. Both parties wish to engage the individual consumer—the Googler, the Facebooker, the Tweeter—on the platform for as long as possible. That helps them in several ways: it maximizes their ad space, allows them to collect more data on the user, and altogether enables them to better target the individual user with the content and ads they think are most relevant to that user.

Of course, the internet platform and the agent of disinformation wish to do this for different reasons. For the internet company, it is all about revenue maximization, whereas the disinformation agent wishes to engage the user with their message, political or otherwise.

We have seen so much evidence of disinformation taking off through social media in just the past few weeks. One particularly shocking and recent example originating on a Polish language site is an account of how agents of the North Atlantic Treaty Organization sprayed chemicals on Poland to harm the well-being of local populations there. That story has not a shred of truth. And in fact, the broader chemtrails conspiracy has time and again been verifiably debunked. But it is an account that gained significant traction in readership on social media just last month. And of course, in this instance we see that there is a strong incentive for disinformation agents to seed unrest and have the people of Poland question whether or not NATO means well toward the Polish nation.

Another thing you note in the report is that many voices have called for increased transparency around digital advertising practices as a solution to these problems, but you suggest that this might not be the sort of panacea that advocates hope for. Could you explain why?

Absolutely. Transparency is a good start to address the scourge of disinformation. The public and governments around the world, including the United States Congress, are increasingly pushing for measures that can ensure greater transparency in political advertising, and in digital advertising more generally. And that would be a big deal, but will it be enough? I do not think so.

Depending on how these transparency initiatives and tools are implemented for political content and advertising, they will possess some potential to inform those people who are proactively interested in understanding patterns of disinformation, including journalists and researchers. But transparency is going to do little to stop disinformation agents from reaching the people that they wish to reach with the messages that they want to spread. We think that the core problem here is the fundamental alignment between the interests of the internet platforms and the disinformation operators, and to truly get at the heart of this issue, we will need to segregate those shared interests.

You also suggested that if transparency exposes a great deal of activity that is questionable but not necessarily illegal or backed by a foreign power, then greater transparency may legitimize these other forms of harmful activity. Is that a concern?

It absolutely is a concern. We don't know the absolute extent of the engagement of political disinformation on social media. There may very well be inordinately more political disinformation that appeared on these platforms than the amount that the social media companies have shared with the public—unbeknownst to them, to be fair. Let me be clear that I'm not saying that big companies are aware of the existence of nefarious disinformation operations and are not revealing it, but just that they may not be aware of it and there is a great deal of it that is happening. This is entirely possible.

And you're exactly right: if it is found that there is inordinately more political disinformation on these social media platforms than what we already know, then it almost becomes a bit of a cesspool. And what can we do with that but just drain it of audience targeting—whether with sponsored or organic content—altogether? Which, of course, is not a viable solution. So your analysis is spot-on. Transparency is certainly not the be all and end all of ceasing the problems of political disinformation.

You wrote that we should view Russian propaganda through a political economic lens in addition to a national security lens, because framing the problem as a national security challenge puts the onus to respond primarily on the national security community. What do we risk missing by privileging the national security response?

It's tremendous that we have leading politicians in the United States now vociferously advocating for changes to stop online disinformation operations. Now, you're right to point out that there is a strong national security theme to their advocacy; they hook the points that they are making to the fact that it is a historically adversarial foreign actor pushing this egregious content and trying to undermine democratic political processes. To date, the public's attention has been so relatively thin on these issues that politicians have had to use the national security argument. But there is a strong commercial and economic aspect to this as well.

This is why, in our report, my co-author Ben Scott and I conduct a market analysis of the digital advertising ecosystem and try to show how the digital economy that our society has created over the past two decades has become the root cause of the tensions that we're seeing surface today in our national political culture. This line of thinking has encouraged the public, the industry, and even the Congress to support measures to shine a light on entities behind political ads, and thereby perhaps identify the agents of disinformation.

That is a good place to start, but it's only a tentative first step. Even with measures around transparency, disinformation will still reach the people that disinformation actors are trying to influence. And so we really need to think about the economic underpinnings of the digital advertising ecosystem. That starts with behavioral data tracking, and moves into online ad-buying and the creation of custom audiences in social media and internet platform advertising, and finally onto search engine optimization and the integration of artificial intelligence throughout all these technologies. And until we address the core of this issue by looking at fundamental reforms to the way that we manage and regulate consumer privacy and autonomy and competition policy in the market, we are not going to see an end to online disinformation operations.

But I will say this as well: going forward, it would be great to see even more advocacy from visible politicians around the world to this effect. And I do believe that that can raise this as an issue in the public's eye and further encourage steps to mitigate the effects of political disinformation.

Your report includes a detailed set of recommendations; I'm most interested in those for civil society activists, whom a 2017 report by Claire Wardle called upon to be honest brokers. Have you seen advocates adopt any promising approaches on this topic?

I would say that Claire is absolutely correct that actors in civil society must be the honest brokers of the discourse going forward. We need to understand the issues on both sides. This requires not only an understanding of the incidents and social problems associated with disinformation operations that can uproot a democratic society, but also the technological and economic constraints of the internet companies that unwittingly are the hosts of disinformation. We all have to do our part.

The only thing I would add here is that of course there are many corners of civil society. Everyone in civil society has a different role. We need people who can take a hard line when advocating to government. We also need people who can listen to the concerns of industry. And finally, we need serious thinkers in the middle who are ready to try to understand what is happening in this ecosystem, consider the arguments of all the policy experts in this arena, and develop a balanced and viable public policy solution moving forward.

I'm curious how you view the idea of norms and self-restraint regarding this issue. During last year's German elections, all but one party agreed to refrain from using automated accounts during the campaign. I'm wondering if down the line it will be possible to develop a 'code of conduct' where responsible actors can manage their behavior. Is that a realistic prospect? What might it look like in practice?

This is a very interesting idea. We have seen codes of conduct adopted in all sectors of the industry, which industry argues do a great job of giving consumers agency in the face of data collection and digital advertising. And those codes of conduct are good in aligning the activities of industry in a way that regulators around the world can enforce.

Now, I'm not implicitly endorsing here any particular code of conduct; I'm highlighting the fact that in certain spheres, these types of codes might have moderate success. In this particular example of adopting and implementing a code of conduct amongst, say, political parties or candidates involved in a national election, in my personal view it seems like a very difficult task, almost an impossible one, for such a code of conduct to be implemented in a way that is stable and fair.

As far as I'm aware, the [German far-right party] *Alternative fur Deutschland* was the sole defector from the German code of conduct and they were quite active on social media and other internet platforms, so there is problem number one. You may not get every actor, and you might have some making the commitment, but what is to say that that collective commitment will have any impact if perhaps the most egregious actor is still engaging in targeted political advertising tactics?

I do think a code like this can potentially work to limit the effects of disinformation, but only if all parties agree to participate. Furthermore, this type of solution says nothing of the limitations that a policy like this might place on the freedom of speech and the freedom of political expression.

Going forward, I think we must permit political advertising on social media. But it is very clear that we require far better standards to assure its ethical implementation and use.

Your report mentioned that in many ways the Russian government seems to have relied on "mediocre tradecraft." Could you give our readers a sense of what you meant by that, and what we might expect more sophisticated threats to look like in the future?

Perhaps the most sophisticated things that Russian disinformation agents did involved targeted advertising and the use of bot armies on social media. These are techniques that any social media user could use. But that's not to say that the Russians who engaged in this activity were not relevant or intelligent. On the contrary, I believe that they were intelligently managing this disinformation campaign in that they knew that these relatively unsophisticated disinformation tactics could and would work. They didn't need to do anything that was particularly high-tech. And that is because of the relative level of sophistication of the targeted advertising and content-curation technologies that are already prevalent on the leading internet platforms.

In the way forward, I think we must account for the further integration of advanced algorithmic technologies throughout this whole digital advertising ecosystem. That includes the further integration of machine learning and artificial intelligence, which I believe will be pushed into the core of the digital advertising technologies that we see on the major platforms today. This is going to mean that the selection and curation of the user audiences, and the matching of content to target them with, is going to increase in precision and accuracy to an extreme degree. And that is without doubt a trend that I do believe sophisticated disinformation agents, including from Russia, but also from other foreign actors and perhaps and even many domestic ones, are studying and will attempt to take advantage of in forthcoming elections around the world.