The New York Times | https://www.nytimes.com/2023/01/15/opinion/ai-chatgpt-lobbying-democracy.html

GUEST ESSAY

How ChatGPT Hijacks Democracy

Jan. 15, 2023

By Nathan E. Sanders and Bruce Schneier
Mr. Sanders is a data scientist. Mr. Schneier is a security technologist.

Launched just weeks ago, ChatGPT is already threatening to upend how we draft everyday communications like emails, college essays and myriad other forms of writing.

Created by the company OpenAI, ChatGPT is a chatbot that can automatically respond to written prompts in a manner that is sometimes eerily close to human.

But for all the consternation over the potential for humans to be replaced by machines in formats like poetry and sitcom scripts, a far greater threat looms: artificial intelligence replacing humans in the democratic processes — not through voting, but through lobbying.

ChatGPT could automatically compose comments submitted in regulatory processes. It could write letters to the editor for publication in local newspapers. It could comment on news articles, blog entries and social media posts millions of times every day. It could mimic the work that the Russian Internet Research Agency did in its attempt to influence our 2016 elections, but without the agency's reported multimillion-dollar budget and hundreds of employees.

Automatically generated comments aren't a new problem. For some time, we have struggled with bots, machines that automatically post content. Five years ago, at least a million automatically drafted comments were believed to have been submitted to the Federal Communications Commission regarding proposed regulations on net neutrality. In 2019, a Harvard undergraduate, as a test, used a text-generation program to submit 1,001 comments in response to a government request for public input on a Medicaid issue. Back then, submitting comments was just a game of overwhelming numbers.

Platforms have gotten better at removing "coordinated inauthentic behavior." Facebook, for example, has been removing over a billion fake accounts a year. But such messages are just the beginning. Rather than flooding legislators' inboxes with supportive emails, or dominating the Capitol switchboard with synthetic voice calls, an A.I. system with the sophistication of ChatGPT but trained on relevant data could selectively target key legislators and influencers to identify the weakest points in the policymaking system and ruthlessly exploit them through direct communication, public relations campaigns, horse trading or other points of leverage.

When we humans do these things, we call it lobbying. Successful agents in this sphere pair precision message writing with smart targeting strategies. Right now, the only thing stopping a ChatGPT-equipped lobbyist from executing something resembling a rhetorical drone warfare campaign is a lack of precision targeting. A.I. could provide techniques for that as well.

A system that can understand political networks, if paired with the textual-generation capabilities of ChatGPT, could identify the member of Congress with the most leverage over a particular policy area — say, corporate taxation or military spending. Like human lobbyists, such a system could target undecided representatives sitting on committees controlling the policy of interest and then focus resources on members of the majority party when a bill moves toward a floor vote.

Once individuals and strategies are identified, an A.I. chatbot like ChatGPT could craft written messages to be used in letters, comments — anywhere text is useful. Human lobbyists could also target those individuals directly. It's the combination that's important: Editorial and social media comments get you only so far, and knowing which legislators to target isn't in itself enough.

This ability to understand and target actors within a network would create a tool for A.I. hacking, exploiting vulnerabilities in social, economic and political systems with incredible speed and scope. Legislative systems would be a particular target, because the motive for attacking policymaking systems is so strong, because the data for training such systems is so widely available and because the use of A.I. may be so hard to detect — particularly if it is being used strategically to guide human actors.

The data necessary to train such strategic targeting systems will only grow with time. Open societies generally make their democratic processes a matter of public record, and most legislators are eager — at least, performatively so — to accept and respond to messages that appear to be from their constituents.

Maybe an A.I. system could uncover which members of Congress have significant sway over leadership but still have low enough public profiles that there is only modest competition for their attention. It could then pinpoint the SuperPAC or public interest group with the greatest impact on that legislator's public positions. Perhaps it could even calibrate the size of donation needed to influence that organization or direct targeted online advertisements carrying a strategic message to its members. For each policy end, the right audience; and for each audience, the right message at the right time.

What makes the threat of A.I.-powered lobbyists greater than the threat already posed by the high-priced lobbying firms on K Street is their potential for acceleration. Human lobbyists rely on decades of experience to find strategic solutions to achieve a policy outcome. That expertise is limited, and therefore expensive.

A.I. could, theoretically, do the same thing much more quickly and cheaply. Speed out of the gate is a huge advantage in an ecosystem in which public opinion and media narratives can become entrenched quickly, as is being nimble enough to shift rapidly in response to chaotic world events.

Moreover, the flexibility of A.I. could help achieve influence across many policies and jurisdictions simultaneously. Imagine an A.I.-assisted lobbying firm that can attempt to place legislation in every single bill moving in the U.S. Congress, or even across all state legislatures. Lobbying firms tend to work within one state only, because there are such complex variations in law, procedure and political structure. With A.I. assistance in navigating these variations, it may become easier to exert power across political boundaries.

Just as teachers will have to change how they give students exams and essay assignments in light of ChatGPT, governments will have to change how they relate to lobbyists.

To be sure, there may also be benefits to this technology in the democracy space; the biggest one is accessibility. Not everyone can afford an experienced lobbyist, but a software interface to an A.I. system could be made available to anyone. If we're lucky, maybe this kind of strategy-generating A.I. could revitalize the democratization of democracy by giving this kind of lobbying power to the powerless.

However, the biggest and most powerful institutions will likely use any A.I. lobbying techniques most successfully. After all, executing the best lobbying strategy still requires insiders — people who can walk the halls of the legislature — and money. Lobbying isn't just about giving the right message to the right person at the right time; it's also about giving money to the right person at the right time. And while an A.I.

chatbot can identify who should be on the receiving end of those campaign contributions, humans will, for the foreseeable future, need to supply the cash. So while it's impossible to predict what a future filled with A.I. lobbyists will look like, it will probably make the already influential and powerful even more so.

Nathan E. Sanders is a data scientist affiliated with the Berkman Klein Center at Harvard University.

Bruce Schneier is a security technologist and lecturer at Harvard Kennedy School. His new book is "A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back."

A correction was made on Jan. 15, 2023*: An earlier version of this article misstated which agency received more than one million automatically drafted comments about proposed regulations on net neutrality. It was the Federal Communications Commission, not the Federal Trade Commission.*