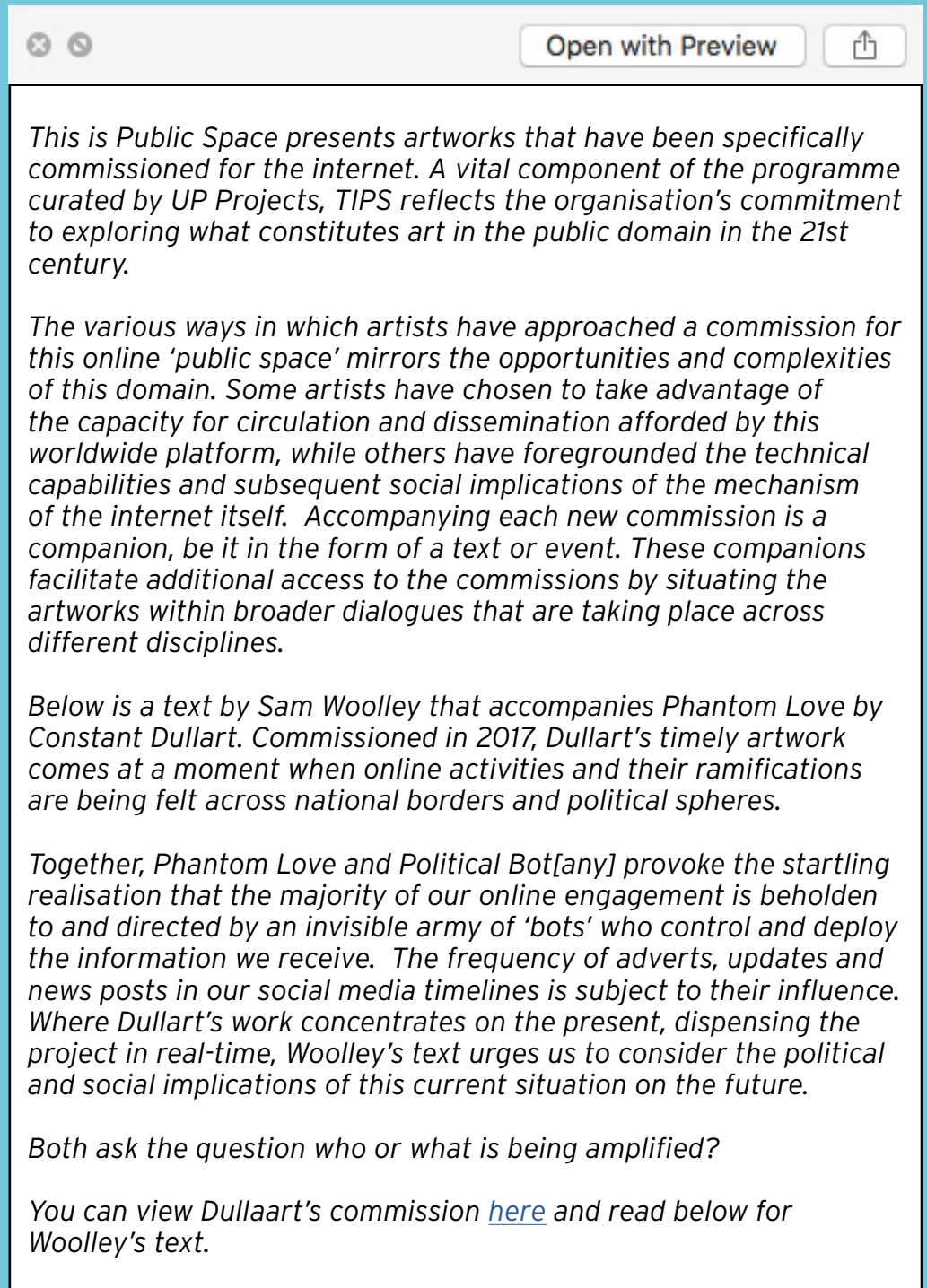


This is Public Space



X CLOSE

IS TH



Swimming

Political Bot[any]: Exploring the Nature of the Social Media Bot

Samuel Woolley

Four and a half years ago several colleagues and I co-founded a research project at the University of Washington in Seattle. Our goal was to gain insight into the ways that bots and automated software were used to do online tasks on behalf of a person for political purposes. More than anything, I wanted to understand the intentions behind using bots for political communication and our team called these creations "political bots." Political bots are automated accounts on social media, constructed to mimic real people in order to manipulate public opinion. How were bots used in for political purposes? Who was using them? Why were they using them? Our team had noticed armies of political bots being deployed over Twitter during the Arab Spring to amplify the standing of particular

← → ↺ Q SAMUEL WOOLLEY

← → ↺ Q SAMUEL WOOLLEY

← → ↺ Q SAMUEL WOOLLEY

← → ↺ Q SAMUEL WOOLLEY

← → ↺ Q SAMUEL WOOLLEY



people or ideas. They would automatically retweet or like messages from particular politicians while simultaneously sending out stock messages on their behalf. At the same time, political bots were being used to stifle conversations amongst democratic activists in North Africa and the Middle East who were attempting to use social media to communicate and organize. Automated accounts would spam the hashtags that groups were using to coordinate, filling them with stock photos and garbled scripts. We knew we were seeing something unusual, but we had no idea that social media bots would become such a crucial tool for manipulating information flows in years to come.

Of course, people around the globe are now aware that a variety of powerful political actors—from the Russian Government to ISIS to campaign managers in Europe and North America, have all used bots in efforts to interrupt and control communication over social media. The U.S. congress highlighted political bots as crucial tools in both foreign intervention and the spread of “fake” news during the 2016 U.S. election. Heads of State in the Philippines, Ecuador, and Turkey have sanctioned the usage of “keyboard armies” and online troll networks that use bots to facilitate the spread of pro-regime propaganda and attacks upon opposition.

While the negative uses of bots tend to dominate stories in the news and media, there has also been growth in using social media bots as social scaffolding: to aid journalists building better one-to-one

WOOLLEY

WOOLLEY

LEY

LEY

OLLEY

connections with readers , to help political activists reach young voters and to allow artists the ability to critique power and express creativity. These uses, and those less palatable, reveal the particular benefits of the bot as a new medium for communication. They also illuminate a unique connection between the bot and the person who builds and launches it. In short, bots act as a proxy for their builders, regardless of whether they are being used to manipulate, uncover, or comment.

Both the proxy nature of bots and their socio-political power as tools are built upon the same categorical foundations that the Atlantic Council's Ben Nimmo says can aid in the detection of manipulative political bots. They are defined by activity, amplification, and anonymity. The average political bot "exist[s] to promote messages" (activity), "hypertweets" (amplification), and lacks a verifiable identity (anonymity). But what do such characteristics mean for bot makers who use bots to produce journalism or create art? What do they mean for current, value-laden, conceptions of bots?

All three markers of the bot can be just as useful to a data-minded reporter as they can to the unethical political communication consultant. One bot building journalist told me that he thinks of his creations as "information radiators" that constantly report on his behalf while he works on other tasks. They can crawl massive data leaks, isolate key points, and release them over Twitter. Unlike their

builders, these bots are able to be constantly active and amplify issues that get lost in mountains for information. Bots make data understandable; connecting NRA to politicians' stances on gun control or releasing the latest scientific information on climate change.

When a reporter launches this kind of social media bot it can give the account legitimacy and allow it to gain followers. It can also make that reporter the target of particular zealous political trolls. The potential characteristic of anonymity is tricky when it comes to using bots for the causes of democracy or creativity. A lack of identity is often a feature of the political bot, but it can also serve to protect journalists and democratic activists using bots as novel means of communication. In fact, one activist told me she built an anonymous bot that argued with trolls in order to keep them busy. She had become so worn down by the constant barrage of hate speech and threats directed at friends, colleagues, and the general public that she decided to use automation as a solution to a problem that was likely facilitated by automation.

In 2015, I co-authored a piece with 13 other bot experts (botanists?) entitled "How to Think About Bots." We wrote that "platforms, governments and citizens must step in and consider the purpose, and future, of bot technology before manipulative anonymity becomes a hallmark of the social bot." In some ways, I think this battle has been lost. The manipulative version of anonymity has become an Achilles

heel for social media firms, regardless of gameable “real-name” policies, because it has allowed their services to become tools for propagandists. In popular media, concerns about bots are now nearly inextricable from a broader lack of transparency over social media and political machinations. The concern now is not just about how anonymous bot accounts might spread mis- or dis- information, it is also about how these digital automatons could unknowingly tweak what users see in their newsfeed or find to be trending.

Anonymity, as ever, is closely tied to privacy and both of these are tied to foundational tenants of democracy. Indeed, conversations with bot makers have made it clear to me that anonymity can be as—and even more—useful to activists who use bots as proxies for protection as they can to political actors who use them to cover their tracks. So where does that leave policymakers trying to regulate the now gargantuan problem of digital disinformation, publics working to decide whether or not a social media trend is manufactured, or tech platforms looking for curb manipulative uses while preserving beneficial ones? What does it mean for the variety of people who use bots in new, and as of yet unforeseen, ways?

It is clear that more regulation of social media is coming, and it will no longer be primarily self-guided by tech firms. As this happens, there will be a desire for those who have cursory understandings of the situation at hand to use bots as a scapegoat. Platforms like Twitter,

which have always had quite open bot policies, are facing the most scrutiny from lawmakers and the public. But it isn't necessarily the use of bots that is the problem. Twitter allowed for bots, at least in part, because it hoped to draw builders making creative uses of software in order to better experiences on the platform. Sadly, the company didn't seem to consider how this access could be exploited.

Automation—along with activity, amplification, and anonymity—can be leveraged in problematic ways in online communication. They can, however, also be useful to groups who have good reasons to fear speaking truth to power. In the United States, at least, attorneys are set to have a field-day over the complex questions relating to how these characteristics of a great deal of digital communication relate to free speech.

One route for addressing the issue of online political manipulation lies in considering not just automation—or another one of the three A's of political bots—but also a variety of other markers of in-organic online social movements. If researchers can isolate metrics for tracking such “astroturf” efforts to spread information than they might be able to prevent computational propaganda attacks before they take hold. Another way to help solve this problem is to build better verification systems for identifying automation into social media. What is stopping Twitter from publically identifying when an account is using automation? People can judge by the content whether or not the

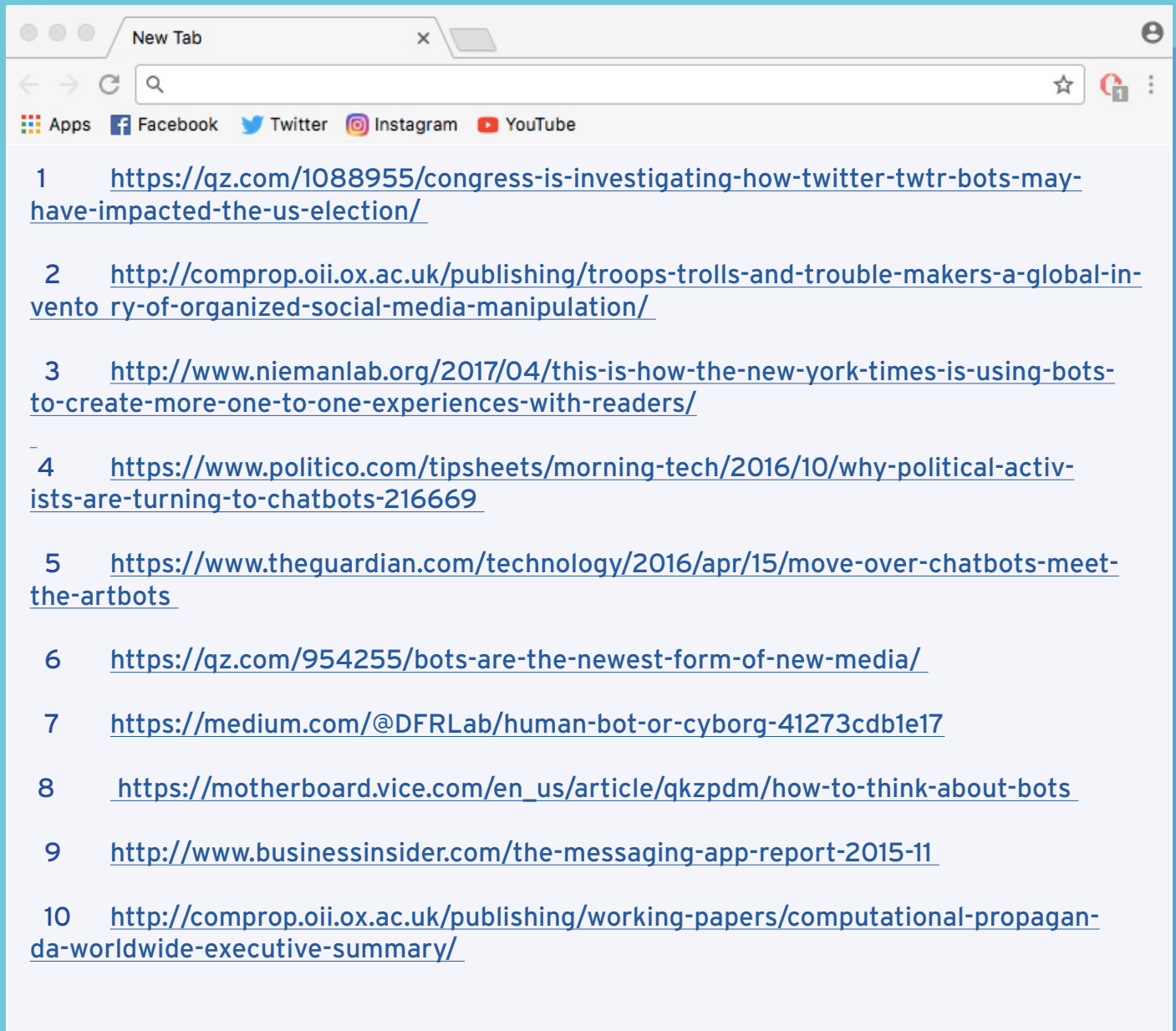
automation is problematic for them and this will help Twitter to isolate accounts that use otherwise acceptable levels automation to spread abuse or junk news.

New digital platforms that seek to close off the ability to propagandize are already emerging. Late last year closed network chat apps like WhatsApp and WeChat overtook traditional social media sites like Facebook and Twitter in terms of monthly active users. However, these platforms are not without their own issues—they still allow for large scale circulation of disinformation and they often lack clear mechanisms for verifying the validity of shared links and stories.

My own research, now based between the Digital Intelligence Lab at the Institute for the Future and the Computational Propaganda Project at the University of Oxford, has made one thing clear: it is time for social media firms to “design for democracy”. We must prioritize the positive social uses of these digital platforms while preventing those that are harmful.



Appendix



Political Bot[Any]: Exploring the Nature of the Social Media Bot

Samuel Woolley

Commissioned by [UP Projects](#)

