Twitter UK
20 Air Street
London
W1B 5AN

twitter.com

24 November 2017

Dear Mr Chairman,

Thank you for your letters dated 19 October and 3 November and for taking time to meet me on the 30th October. I have been asked to reply to your letters in my capacity as Head of Public Policy for Twitter in the UK.

We have now also received a written request for information from the Electoral Commission, which we understand has also been sent to other companies, as part of their investigation into campaign activity during the regulated period for the June 2016 EU Referendum.

We are currently undertaking investigations into these questions and intend to share our findings in the coming weeks.

It is important to note that not all automated accounts are bad, whether posting air quality sensor readings or posting details of Wikipedia edits, while not all high activity accounts are bots. Equally, given Twitter's central control - users choosing to follow or unfollow an account to curate what appears in their timeline- is a robust defence against low-quality automated accounts.

We do not underestimate the importance or complexity of these issues. We have recently published more information about our approach to automated traffic, including:

- On average, our automated systems catch more than 3.2 million suspicious accounts globally per week — more than double the amount we detected this time last year.
- We have built systems to identify suspicious attempts to log in to Twitter, including signs that a login may be automated or scripted. These techniques now help us catch about 450,000 suspicious logins per day.
- Much of this defensive work is done through machine learning and automated processes on our back end, and we have been able to significantly improve our automatic spam and bot-detection tools, resulting in a 64% year-over-year increase in suspicious logins we're able to detect.

Twitter UK
20 Air Street
London
W1B 5AN

twitter.com

- We are committed to combatting the minority of apps that create spam and abuse via our API. Since June 2017, we've suspended more than 117,000 malicious applications for abusing our API, collectively responsible for more than 1.5 billion low-quality Tweets this year.

Recently, there has been increased press coverage of several pieces of research into these issues on Twitter. We remain proud to be a platform that allows open access for academics, indeed recently taking steps to make more data available through a lower-cost premium API. However, we have found studies of the impact of bots and automation on Twitter necessarily and systematically under-represent our enforcement actions because these defensive actions are not visible via our APIs, and because they take place shortly after content is created and delivered via our streaming API.

Furthermore, researchers using an API often overlook the substantial in-product features that prioritize the most relevant content. Based on user interests and choices, we limit the visibility of low-quality content using tools such as Quality Filter and Safe Search -- both of which are on by default for all of Twitter's users and active for more than 97% of users.

Indeed, media reports have recently highlighted how users named as bots in research were real people, reinforcing the risks of limited data being used to attribute activity, particularly in the absence of peer review. We at Twitter are mindful of the implications of a person being falsely accused of being a bot or associated with state-sponsored election interference, and take very seriously our obligations to protect user privacy and safety.

We recognise these issues and are already engaged in dialogue with academics and think tanks around the world, including those in the UK, to discuss potential collaboration and to explore where our own efforts can be better shared without jeopardizing their effectiveness or user privacy.

Finally, I would note that the City University report you cited in your letter of 30 October concludes:

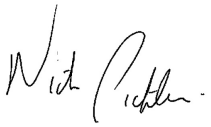
Twitter UK
20 Air Street
London
W1B 5AN

twitter.com

"Despite the botnet's capacity to rapidly trigger such cascades, we have not found evidence supporting the notion that bots can substantively alter campaign communication, as the activity of the botnet—at least of this defunct botnet in particular—was relatively minor with respect to the larger conversation about the referendum that took place on Twitter."

We look forward to answering your questions and working with you in the coming months.

Yours sincerely,



Nick Pickles

Head of Public Policy
Twitter UK