

RON JOHNSON, WISCONSIN, CHAIRMAN

JOHN MCCAIN, ARIZONA  
ROB PORTMAN, OHIO  
RAND PAUL, KENTUCKY  
JAMES LANKFORD, OKLAHOMA  
MICHAEL B. ENZI, WYOMING  
KELLY AYOTTE, NEW HAMPSHIRE  
JONI ERNST, IOWA  
BEN SASSE, NEBRASKA

THOMAS R. CARPER, DELAWARE  
CLAIRE McCASKILL, MISSOURI  
JON TESTER, MONTANA  
TAMMY BALDWIN, WISCONSIN  
HEIDI HEITKAMP, NORTH DAKOTA  
CORY A. BOOKER, NEW JERSEY  
GARY C. PETERS, MICHIGAN

# United States Senate

COMMITTEE ON  
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS  
WASHINGTON, DC 20510-6250

CHRISTOPHER R. HIXON, STAFF DIRECTOR  
GABRIELLE A. BATKIN, MINORITY STAFF DIRECTOR

September 8, 2016

Jack Dorsey  
Chief Executive Officer  
Twitter, Inc.  
355 Market Street Suite 900  
San Francisco, CA 94103

Dear Mr. Dorsey:

I write today regarding troubling reports that Russian state actors may be engaging in covert operations aimed at undermining the political process in the United States. I ask for your assistance in identifying the nature and extent of any such operations on your platform and any steps that may be necessary to protect our democracy from these potential threats.

As has been publicly reported, U.S. intelligence and law enforcement officials are reviewing whether Russia is engaged in active measures to influence the American political process, including through cyberattacks on election systems and propaganda campaigns.<sup>1</sup> This review comes in the wake of reports indicating that the Russian Federal Security Service and Russian military intelligence may have been involved in the recent cyberattacks against the Democratic National Committee and other American political organizations. If these reports are accurate, such activities raise serious concerns about the interference of foreign actors in the American political process during the upcoming election.

Public reports also suggest that Russian state actors may be involved in a coordinated effort to influence public opinion through the malicious use of Twitter and other social networking services.<sup>2</sup> These “social” cyberattacks are made possible through the proliferation of “bots,” automated and often false accounts controlled by a single entity, that pollute information streams by generating messages that appear to come from many different users.<sup>3</sup> According to Twitter’s past filings with the Securities and Exchange Commission, approximately 16 million Twitter users or less—or 5 percent of all users—are false or spam accounts, and the actual number of false or spam accounts could be higher than this estimate.<sup>4</sup>

Indeed, the use of bots on social networking services that allow malicious actors to spread disinformation is well-documented in political campaigns outside the United States.<sup>5</sup> Accordingly, the

---

<sup>1</sup> Dana Priest, Ellen Nakashima & Tom Hamburger, *U.S. Investigating Potential Covert Russian Plan to Disrupt National Elections*, WASHINGTON POST (Sep. 5, 2016).

<sup>2</sup> Adrian Chen, *The Agency*, N.Y. TIMES MAGAZINE (Jun. 2, 2015); Adrian Chen, *The Real Paranoia-Inducing Purpose of Russian Hacks*, THE NEW YORKER (July 27, 2016).

<sup>3</sup> Rebecca Goolsby, *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack*, THE WILSON CENTER (Mar. 4, 2013).

<sup>4</sup> Twitter, Quarterly Report (Form 10-Q) (June 30, 2016).

<sup>5</sup> Jordan Robertson, Michael Riley & Andrew Willis, *How to Hack an Election*, BLOOMBERG BUSINESSWEEK (Mar. 31, 2016).

Department of Defense's Defense Advanced Research Projects Agency has recognized the risk of this activity on social networking services pose to the democratic process and has sponsored efforts to create analytical tools to detect and address covert attempts to manipulate public opinion.<sup>6</sup>

In the past, Twitter has taken substantial steps to address other types of malicious actors on its platform, including suspending 360,000 accounts since the middle of 2015 to enforce its prohibition on violent threats and the promotion of terrorism.<sup>7</sup> This work is commendable and it is something that I know poses unique technical and resource challenges as you and your team combat violent extremism while maintaining an open platform for legitimate users to share their views freely.

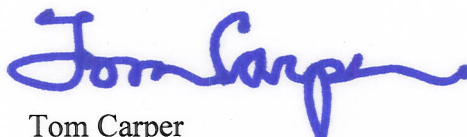
Cybersecurity remains one of our nation's biggest security challenges, and attempts by foreign state actors to covertly interfere the American election through "social" cyberattacks and other efforts would be unacceptable. To better understand the possible use of bots by malicious actors on your platform, I ask that you please provide the following information by September 30, 2016:

1. Please describe the methodology Twitter uses to estimate the number of false or spam accounts and the types of judgment used in this determination. Please also describe whether Twitter has the ability to track or estimate the number of false or spam accounts controlled by potential Russian state actors.
2. Would efforts of Russian state actors to create serial or bulk accounts for disruptive or abusive purposes be prohibited by Twitter's terms of service? If so, please describe the efforts of Twitter to address this problem and actions you've taken to suspend or terminate these types of accounts.
3. Please describe how Twitter invests its resources to reduce bots on the platform, including any bots you suspect may be controlled by Russian state actors, if any.

In addition, I ask that you make representatives from your company available to brief my staff on this issue. Thank you for your attention to this matter.

With best personal regards, I am

Sincerely yours,



Tom Carper  
Ranking Member

cc: The Honorable Ron Johnson  
Chairman

---

<sup>6</sup> V.S. Subrahmanian, et. al, The DARPA TWITTER BOT CHALLENGE, (last updated Apr. 21, 2016).

<sup>7</sup> *An Update on Our Efforts to Combat Violent Extremism*, TWITTER (Aug. 18, 2016).