

September 4, 2018

The Honorable Richard Burr
Chairman
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

The Honorable Mark Warner
Ranking Member
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Ranking Member Warner:

We write regarding the hearing on “Foreign Influence Operations’ Use of Social Media Platforms” to express EPIC’s ongoing concern about the ability of foreign actors to influence American public discourse and democracy through the use of social media platforms. EPIC has sent similar statements regarding Russian interference in the U.S. election to several Senate and House committees.¹

EPIC is a public-interest research center established in 1994 to bring attention to pressing privacy and civil liberties issues.² Following reporting that Russia actively interfered with the 2016 presidential elections, EPIC launched a new project on Democracy and Cybersecurity.³ As part of this effort, EPIC has pursued several Freedom of Information Act (FOIA) cases to help determine the full extent of Russian interference in U.S. elections.⁴ The Committee may be particularly interested in documents obtained through one such case, *EPIC v. FBI*,⁵ that detail FBI victim-notification procedures. These documents, though heavily redacted, are of particular interest after subsequent media reports showed that the FBI not only failed to notify U.S. victims of foreign cyberattacks, but also refused to answer questions about that deviation or provide any meaningful transparency into its process.⁶

The full extent of Russian interference in U.S. elections is still unknown to the public. An early 2017 report from the Intelligence Community (IC) first described the “multi-pronged” attack

¹ See, e.g. Letter to U.S. Senators Burr and Warner regarding Policy Responses to Russian Interference in the U.S. Election (June 19, 2018), <https://epic.org/testimony/congress/EPIC-SSCI-EPICvFBI-June2018.pdf>; Letter to U.S. Representatives Nunes and Schiff regarding Russian Active Measures Investigation (Mar. 20, 2017), <https://epic.org/testimony/congress/EPIC-HPSCI-Russia-Mar2017.pdf>.

² EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

³ See EPIC, *Democracy and Cybersecurity*, <https://epic.org/democracy>.

⁴ *EPIC v. ODNI*, 281 F.Supp.3d 203 (D.D.C. 2017); *EPIC Seeks Release of FISA Order for Trump Tower*, EPIC (Mar. 6, 2017), <https://epic.org/2017/03/epic-seeks-release-of-fisa-ord.html>; *EPIC v. IRS*, No. 17-670 (D.D.C. filed Apr. 15, 2017).

⁵ *EPIC v. FBI*, 2018 U.S. Dist. LEXIS 85467 *; 2018 WL 2324084 (D.D.C. May 22, 2018); *EPIC v. FBI* (Russian Hacking), <https://epic.org/foia/fbi/russian-hacking>.

⁶ *FBI Deviated from Policy on Notifying Victims of Russian Hackers, Report Says*, CBS NEWS (Nov. 27, 2017), <https://www.cbsnews.com/news/ap-investigation-russia-hackers-phishing-emails-fbi-policy>.

on US election.⁷ New information has since surfaced leading to this Committee’s findings that Russian efforts extended far beyond those initially reported by the IC.⁸ This Committee found that “Russian effort to manipulate social media outlets” was “far more extensive” than acknowledged in the IC report.⁹ Further, the Committee’s report found a much greater level of interference with state and local elections than were described in the IC report, including that operations “likely aimed at preparing to discredit the integrity of the U.S. voting process” had begun “at least” as early as 2014.¹⁰

The American public still does not have the full picture on Russian interference. To be sure, even the social media companies whose systems were exploited do not appear to have a full grasp of the influence exerted through their platforms: as late as this summer, both Facebook and Twitter were discovering and deleting new fake accounts, many linked to similar influence campaigns.¹¹ The public deserves a full accounting of the challenges it faces from foreign influence operations, both from the IC and from the social media platforms that provide the means for foreign actors to peddle their poisonous ideologies.

Nevertheless, the IC and major social media platforms have provided little in the way of transparency. The witnesses appearing before you tomorrow should address these concerns.¹² We therefore urge you to encourage them to be fully transparent with the public about their efforts to combat foreign influence operations. Specifically, EPIC recommends that you question the witnesses about:

- What steps, if any, the companies take to ensure that extremist or potentially damaging content is not privileged or promoted by search algorithms or paid advertising;
- What strategies, other than removal, the companies employ to ensure that foreign influence operations do not successfully employ their platforms;

⁷ OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf
https://www.dni.gov/files/documents/ICA_2017_01.pdf. EPIC sued under the Freedom of Information Act for the release of the complete report. *EPIC v. ODNI*, 281 F.Supp.3d 203 (D.D.C. 2017); *See also EPIC v. ODNI* (Russian Hacking), <https://www.epic.org/foia/odni/russian-hacking>.

⁸ Senate Select Committee on Intelligence, *The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections—Summary of Initial Findings* (July 3, 2018), <https://www.intelligence.senate.gov/publications/committee-findings-2017-intelligence-community-assessment>.

⁹ *Id.*

¹⁰ Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations* (May 8, 2018), <https://www.intelligence.senate.gov/publications/russia-inquiry>.

¹¹ Issi Lapowsky, *Fake Facebook Accounts Are Getting Harder to Trace*, WIRED (July 31, 2018), <https://www.wired.com/story/facebook-uncovers-new-fake-accounts-ahead-of-midterm-elections>; Nicholas Confessore & Gabriel J.X. Dance, *Battling Fake Accounts, Twitter to Slash Millions of Followers*, N.Y. TIMES (July 11, 2018), <https://www.nytimes.com/2018/07/11/technology/twitter-fake-followers.html>.

¹² For instance, Facebook recently released its community guidelines, explaining how content moderation choices are made. Further information on this process from Facebook and Twitter would provide significant transparency about the platforms’ efforts to curtail foreign influence in U.S. politics. *See Facebook, Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process* (Apr. 24, 2018), <https://newsroom.fb.com/news/2018/04/comprehensive-community-standards>.

- What steps, if any, the companies have taken to ensure that the increasing number of bots employing sophisticated natural-language processing are not used to harm the U.S. electoral process or other democratic institutions;
- How their companies ensure that they do not block or bury legitimate political debate in the process of ensuring foreign influence operators do not disrupt the U.S. democratic process;
- Whether their companies are willing to collaborate and share information with each other about confirmed bad actors, and if not, why not;
- How their companies ensure that responses to foreign election meddling do not harm other goals, such as algorithmic transparency and free speech;
- What, if any, activity, the companies have seen that suggests foreign operators may be intending to interfere with the November 2018 midterm elections.

With midterm elections rapidly approaching, the need to fully understand the extent of foreign intelligence operators' influence on U.S. elections is more critical than ever. EPIC appreciates your ongoing efforts on this issue and look forward to continuing to work with the Committee to provide full answers to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Jeff Gary
Jeff Gary
EPIC Legislative Fellow