DATE: December 13, 2017

TO: Ajit Pai, Chairman, FCC
Mignon Clyburn, Commissioner, FCC
Michael O’Rielly, Commissioner, FCC
Brendan Carr, Commissioner, FCC
Jessica Rosenworcel, Commissioner, FCC

FROM: Charles Belle, Executive Director, Startup Policy Lab
CC: Gina Cooper, Programming Director, Startup Policy Lab

RE: Truth in Public Comments Research
FCC’s Restoring Internet Freedom (Docket FCC-17-108) Proceeding

Chairman Pai and Commissioners:

In response to the growing concerns of scientific and legal communities, Startup Policy Lab (SPL), a 501(c)3 nonprofit think tank, commissioned the Truth in Public Comments (TiPC) research project to examine the veracity of public comments submitted to the Federal Election Commission’s (FCC) website regarding the FCC’s Restoring Internet Freedom (Docket FCC-17-108) Proceeding.

Attached please find a preliminary report documenting our findings. This report, along with all supporting data (with personally identifiable information purged) will be published for the public to examine.

Our methodology was straightforward. We used the FCC API to download public comment data, selected a random sample of over 450,000 public comments and emailed a simple question:

Did you submit the comment quoted below to the FCC, yes or no?

Over 14,000 people answered the question, and the results were alarming.

88% of survey respondents whose emails were used to submit pro-repeal comments replied, “no,” that they did not submit the comment. Conversely, only 4% of pro-net neutrality respondents said that they did not submit the comment attributed to them.

We believe this indicates a deliberate attempt to interfere with the FCC’s public comment process. The systemic attack and overwhelming numbers indicate a high level of intent and resourcefulness that employs an understanding of how information flows through government.
These findings are relevant to any governmental agency (Federal, State, or Local) that receives public comments. These findings should be treated as early evidence of threats to the systems of democracy that impact all citizens.

We also believe that we are observing an evolution in cyber-aggression where the target of propaganda is government itself. And while this is certainly frightening, it is also an opportunity. Both the breach and evidence are on government servers, and the data logs and other information needed to further investigate this fraud against our government, is already in the hands of the FCC.

We concur with others that more information is needed to understand the nature of the threat in order to develop safeguards. Further study is required to implement legal and technical processes that prevent malicious efforts to undermine citizen confidence in democratic processes.

We encourage the FCC to take immediate steps to investigate this act of bot-driven fraud.

Sincerely,

Charles Belle
Executive Director
Startup Policy Lab