Graphika

RESPONSES TO QUESTIONS FOR THE RECORD
For Senate Select Committee on Intelligence: Foreign Influence Operations and Their Use of Social Media Platforms
Dr. John W. Kelly, Chief Executive Officer
August 30, 2018

Answers for Senator Cotton

Dear Senator Cotton,

I fully agree that current Russian propaganda leverages tactics and themes familiar to history professors. In that regard, it is indeed "old wine." What is new is that in 2018, we manufacture and distribute the bottles. And we do so with a distribution system that is far more effective at delivering tailored Russian messages to specific American audiences.

Contemporary Russian propaganda is distributed to US audiences on American social media platforms, and through American companies. There are both new risks and new opportunities in this scenario. The primary risk is that, as these Russian manipulation strategies are exposed and denounced, American businesses suffer the cost of having been so blatantly manipulated. The opportunity is that, properly harnessed, we can leverage platform data to achieve unprecedented insight into the details of operations designed to manipulate American audiences. As Facebook's recent proactive disclosures show, the current state of affairs enables the ability to detect and disclose influence campaigns before they have an opportunity to further spread.

Answers for Senator Manchin

Dear Senator Manchin,

Foreign influence campaigns on social media are rarely constrained within a single platform, and sophisticated actors are adept at covering their tracks. There is no Russian team with a "Facebook" assignment: rather, we now know (thanks to the excellent academic efforts and investigative journalism in this space) that teams are empowered to influence specific topics (such as the efficiency of vaccines) or audiences (such as African-American activists), and to leverage *all* necessary channels and platforms in doing so.

As a result, large social media companies must cooperate with one another and also empower external experts to detect manipulations and help them understand how they are being

"gamed" by foreign actors and others leveraging similar techniques. This is a problem for the entire technology industry, and it won't be solved in silos constrained by each platforms' specific features and products.

Digital watermarking and other techniques for creating audit trails for content origin might provide some value within a larger strategy, but these alone would prove little more than a speed-bump to manipulators. Alone, these are lightweight "tree solutions," forensics assessments that focus on only one simple aspect of the problem. *Is this tree real or plastic?* In the coming arms race for 21st Century cyber-social warfare, we require "forest solutions," approaches that employ sophisticated large-scale data analysis to detect manipulation at scale across multiple channels and platforms.

We believe that an investment in research and development in this space will yield efficient methods for the detection of foreign manipulation and that those methods will be - as they must be - consistent with American values regarding the protection of user privacy.

Answers for Senator King

Dear Senator King,

Thank you for raising this question, which is focused on the many solutions needed to tackle foreign disinformation. Allow me to reply primarily on the technical front, which is my principal area of expertise.

Leveraging Federal research grants, academic partnerships, and private partnerships with the best and brightest in Silicon Valley, Graphika has already made significant headway in developing frameworks to detect and identify inorganic coordination and messages amplified by both automated and human (bot and troll) online armies. This is not a simple problem, and solving it requires significant investment in network science R&D.

For many years, the detection problem was solely focused on "bots": automated scripts posting social media messages with minimal human intervention. Today, we recognize the problem is more complex than simple automation. Foreign actors, and a growing black market serving their efforts, have developed many techniques to inorganically amplify social media signals in manners more subtle (and harder to detect) than simple bots. This is what Graphika and our partners are mostly focused on now.

Doing this work properly will require that the platforms continue to facilitate access to the types of data needed for researchers and innovators to conduct these analyses and generate new detection models, while ensuring user privacy remains protected.