Written Testimony of Kent Walker
Senior Vice President and General Counsel, Google
House Permanent Select Committee on Intelligence
Hearing on "Russia Investigative Task Force Hearing with Social Media Companies"
Written Congressional Testimony
November 1, 2017

Chairman Nunes, Ranking Member Schiff, and members of the Committee, thank you for the opportunity to appear before you this morning.

My name is Kent Walker. I am Senior Vice President and General Counsel at Google and I lead our Legal, Policy, Trust and Safety, and Philanthropy teams. I've worked at the intersection of technology, security, and the law for over 25 years, including a tour early in my career as an Assistant US Attorney at the Department of Justice focusing on technology crimes.

We believe that we have a responsibility to prevent the misuse of our platforms and we take that very seriously. Google was founded with a mission to organize the world's information and make it universally accessible and useful. The abuse of the tools and platforms we build is antithetical to that mission.

Google is deeply concerned about attempts to undermine democratic elections. We are committed to working with Congress, law enforcement, others in our industry, and the NGO community to strengthen protections around elections, ensure the security of users, and help combat disinformation.

We are dealing with difficult questions that balance free expression issues, unprecedented access to information, and the need to provide high quality content to our users. There are no easy answers here, but we are deeply committed to getting this right. We recognize the importance of this Committee's mandate, and we welcome the opportunity to share information and talk about solutions.

Of course disinformation and propaganda campaigns aren't new, and have involved many different types of media and publications. When it comes to online platforms, for many years we have seen nation states and criminals attempt to breach our firewalls, game our search results, and interfere with our platforms. These attempts range from large-scale threats, such as distributed denial of service attacks, which we are able to identify and thwart quickly, all the way down to small-scale, extremely targeted attacks, such as attempts to gain access to email accounts of high-profile individuals.

We take these threats very seriously. We serve billions of users every day, so our solutions need to work at scale. We've built industry-leading security systems and we've put these tools into our consumer products. Back in 2007, we launched the first version of our Safe Browsing tool, which helps protect users from phishing, malware, and other attack vectors. Today, Safe Browsing is used on more than three billion devices worldwide. If we suspect that users are subject to government-sponsored attacks we warn them. And last month, we launched our Advanced Protection Program, which integrates physical security keys to protect those at greatest risk of attack, like journalists, business leaders, and politicians. We face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats.

Our tools don't just protect our physical and network security, but also detect and prevent artificially boosting content, spam, and other attempts to manipulate our systems. On Google News, for example, we label links so users can see if the content is locally sourced, an OpEd, or an in-depth piece. For Google Search, we have updated our quality guidelines and evaluations to help identify misleading information, helping surface more authoritative content from the web. We have updated our advertising guidelines to prohibit ads on sites that misrepresent themselves. And on YouTube we employ a sophisticated spam and security-breach detection system to detect anomalous behavior and catch people trying to inflate view counts of videos or numbers of subscribers.

We have deployed our most advanced technologies to increase security and fight manipulation, but we realize that no system is going to be 100% perfect. It is hard to rapidly identify all untruthful content at massive scale, and harder yet to understand the motives and potential connections of the people posting that content. But we have made substantial progress

in preventing and detecting abuse, and we are seeing continued success in stopping bad actors attempting to game them. And as threats evolve, we will continue to adapt in order to understand and prevent new attempts to misuse our platforms.

With respect to the Committee's work on the 2016 election, we have looked across our products to understand whether individuals apparently connected to government-backed entities were using those products to disseminate information with the purpose of interfering with the US election. We based this review on research into misinformation campaigns from Alphabet's Jigsaw group, our information security team's own methods, and leads provided by other companies.

While we did find activity associated with suspected government-backed accounts, that activity appears to have been limited on our platforms. Of course, any activity like this is more than we would like to see. We have provided the relevant information to the Committee, have issued a public summary of the results of our review, and will continue to cooperate with the Committee's investigation.

Starting with our ads products, we found two accounts that appear to be associated with this effort. These accounts spent approximately $4700 dollars in connection with the 2016 presidential election, representing less than 0.0002 percent of the total amount spent on that race. We believe that the activity we found was limited because of various safeguards that we had in place in advance of the 2016 election, and the fact that Google's products didn't lend themselves to the kind of micro-targeting or viral dissemination that these actors seemed to prefer.

As part of our investigation, we also looked at our other services. Let me share a few key points. On YouTube, we did find 18 channels on YouTube with roughly 1,100 videos, a total of 43 hours of content, uploaded by individuals who we suspect are associated with this effort and which contained political content. That compares with the 400 million hours of YouTube content uploaded every minute, and the over one billion hours of YouTube content watched every day. These videos generally had very low view counts; only around 3% percent had more than 5,000 views. The videos were not targeted to any particular sector of the US population as

that's not feasible on YouTube. Additionally, we found a limited number of Gmail accounts that appear to have been primarily used to to set up accounts on social media platforms.

We continue to expand our use of cutting-edge technology to protect our users and will continue working with governments to ensure that our platforms aren't used for nefarious purposes.

We will also be making political advertising more transparent, easier for users to understand, and even more secure.

- In 2018 we'll release a transparency report for election ads, sharing data about who is buying election ads on our platforms and how much money is being spent. We'll pair our transparency report with a database of election ad creatives from across our ads products. And we will make the database available for public research.

- We're also going to make it easier for users to understand who bought the election ads they see on our networks. Going forward, users will be able to find the name of any advertiser running an election ad on Search, YouTube, and the Google Display Network with one click on an icon above the ad.

- We will continue enhancing our existing safeguards to ensure that we only permit US nationals to buy US election ads. We already tightly restrict which advertisers can serve ads to audiences based on their political leanings. Moving forward, we'll go further by verifying the identity of anyone who wants to run an election ad or use our political-interest-based tools and confirming that person is permitted to run that ad.

We certainly can't do this alone. Combating disinformation campaigns requires efforts from across the industry. We'll continue to work with other companies to better protect the collective digital ecosystem, and, even as we take our own steps, we are open to working with governments on legislation that promotes electoral transparency.

Our commitment to addressing these issues extends beyond our services. Google has supported significant outreach to increase security for candidates and campaigns across the

United States, France, Germany, and other countries. We've offered in-person briefings and introduced a suite of digital tools designed to help election websites and political campaigns protect themselves from phishing, unauthorized account access, and other digital attacks. We've partnered with the National Cyber Security Alliance to fund and advise on security training programs that focus specifically on elected officials, campaigns, and staff members. We are also increasing our long-standing support for the bipartisan Defending Digital Democracy Project at the Belfer Center for Science and International Affairs at Harvard Kennedy School.

Let me conclude by recognizing the importance of the work of this Committee. Our users, advertisers, and creators must be able to trust in their security and safety. We share the goal of identifying bad actors who have attempted to interfere with our systems and abuse the electoral process. We look forward to continued cooperation, both with the members of this Committee and with our fellow companies, to both provide access to tools that help citizens express themselves while avoiding abuses that undercut the integrity of elections.

Thank you for the opportunity to tell you about our ongoing efforts in this space. We look forward to continuing to work with Congress on these important issues, and I'm happy to answer any questions you might have.