Written Testimony of Kent Walker

Senior Vice President, Global Affairs & Chief Legal Officer

Senate Select Committee on Intelligence

Hearing on, “Foreign Influence Operations’ Use of Social Media Platforms”

Written Congressional Testimony

September 5th, 2018

Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for the opportunity to provide an update on the efforts we’re making to secure our platforms ahead of the 2018 midterm elections in the US and for future elections around the world.

My name is Kent Walker. I am Senior Vice President, Global Affairs and Chief Legal Officer at Google, and I lead our Legal, Policy, Trust and Safety, and Google.org teams. I’ve worked at the intersection of technology, security, and the law for over 25 years, including time spent 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.

In my testimony to the Committee last fall, I described the investigation we had conducted to understand whether individuals apparently connected to government-backed entities were using our products to disseminate information with the purpose of interfering with the 2016 US election. We based that review on research into misinformation campaigns from our Jigsaw group, our information security team’s own methods, and leads provided by other companies. We identified limited activity and we took swift action, disabling any accounts we found.

We have continued our efforts and work diligently to identify and remove actors from our products who mislead others regarding their identity. We've continued to investigate activity by the Internet Research Agency and other Russia-affiliated entities since we testified before the Committee last year. When we have found activity, we've removed the relevant accounts. We've also investigated activity linked to Iranian influence efforts, similarly removing the accounts we have linked to that activity. We recently issued an updated summary of the results of our review, and are happy to continue to provide our findings to Congress, law enforcement, and our peers. While the activity on our products remains limited, any activity like this is more than we would like to see. We will continue to invest resources to address this issue and to work with law enforcement, Congress, and other companies.

Google remains deeply concerned about attempts to undermine democratic elections. As we promised the Committee last year, we have now fulfilled all four of our commitments to provide increased transparency in election advertising:

First, we've rolled out a **Verification Program** for anyone who wants to purchase a federal election ad on Google in the U.S. We now require that advertisers provide government-issued identification information and other key information to confirm they are a U.S. citizen or lawful permanent resident or a U.S.-based organization, as required by law.

Second, to help people better understand who is paying for an election ad we've incorporated **In-ad Disclosures,** which means we now identify by name advertisers running election-related campaigns on Search, YouTube, Display and Video 360, and the Google Display Network.

Third, we have launched a "Political advertising on Google" **Transparency Report** for election ads, which provides data about the entities buying election-related ads on our platforms, how much money is spent across states and congressional districts on such ads, and who the top advertisers are overall. The report also shows the keywords advertisers have spent the most money on ads of political importance during the current U.S. election cycle from May 31st, 2018 onwards.

Finally, we now offer a **searchable election Ad Library** within our public Transparency Report which shows things like which ads had the highest views, what the latest election ads running on our platform are, and deep dives into specific advertisers' campaigns. The data shows the overall amount spent and number of ads run by each election advertiser, and whether the advertiser targeted its ad campaigns geographically or by age or gender, as well as the approximate amount spent on each individual ad, the approximate impressions generated by each ad, and the dates each ad ran on our platform. In addition, the data from the report and Ad Library is publicly available through Google Cloud's BigQuery. Using BigQuery's API, anyone can write code and run their own unique queries on this data set. Researchers, political watchdog groups and private citizens can use our data set to develop charts, graphs, tables or other visualizations of political advertising on Google Ads services. Together with the Transparency Report, these tools provide unprecedented, data-driven insights into election ads on our platform. We're updating the Transparency Report and Ad Library every week, so as we head into election season, anyone can see new ads that get uploaded or new advertisers that decide to run Google ads.

In addition to our transparency efforts, we have implemented a number of initiatives to improve the cybersecurity posture of candidates, campaigns, and the election infrastructure writ large.

First, in October 2017, we unveiled the **Advanced Protection Program**, which provides the strongest account protection that Google offers. The Advanced Protection Program is designed to thwart targeted spearphishing attacks; it is designed for users that may need an extra layer of protection against such attacks. This includes elected officials and candidates for public office. We have made continuous improvements to the Advanced Protection Program since I last testified before this Committee, including adding support for iOS and making it easier for interested users to purchase security keys. We have conducted extensive outreach to campaigns, candidates, journalists, and human rights activists to help drive use of security keys that are at the heart of the Advanced Protection Program.

Second, in May 2018, Jigsaw, our incubator dedicated to building technology to address significant security challenges, announced the availability of **Project Shield** to U.S. political organizations (e.g., candidates, campaigns, political action committees) registered with the appropriate electoral authorities. Project Shield is a free service that uses Google technology to prevent distributed denial of service (DDoS) attacks that block access to content. DDoS attacks can threaten the integrity of elections by depriving citizens of important information about candidates and elections, and we have seen an increase in such attacks over time. Project Shield is now protecting a diverse array of political organizations. Project Shield also protects state, county, and local electoral board and voter information sites. Google's and Jigsaw's Protect Your Election site provides further information on the tools and resources we have made available to help campaigns, election officials, and news organizations defend against digital attacks.

Third, we **continue to issue warnings to users** when we believe they are at risk of state-sponsored efforts to hijack their accounts. We have issued these warnings for many years, and we will continue to do so in light of account hijacking campaigns we see from state-sponsored actors during this election cycle.

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. Our algorithms are designed to identify content that many people find relevant and useful. We are constantly looking to find signals that help us identify deceptive content, while promoting content that is authoritative, relevant, and current. We have made substantial progress in preventing and detecting abuse, and are seeing continued success in stopping bad actors attempting to game our systems. And as threats evolve, we will continue to adapt in order to understand and prevent new attempts to misuse our platforms.

We certainly can't do this important work 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 partnered with the National Cyber Security Alliance to help promote better account security, which includes security training programs that focus specifically on elected officials and staff members. We also continue to support the bipartisan Defending Digital Democracy Project at the Belfer Center for Science and International Affairs at Harvard Kennedy School. And in 2007, we launched the first version of our Safe Browsing tool, which helps protect users from phishing, malware, and other attack vectors by examining billions of URLs, software, and website content. We have made this tool free and publicly available to webmasters and developers so that they can protect their websites and applications from malicious actors. Today, Safe Browsing is used on more than three billion devices worldwide.

Let me conclude by recognizing the important 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 others in the security community and the broader industry, to provide tools that help citizens express themselves and to address abuses that undercut the integrity of elections.

Thank you for the opportunity to outline our ongoing efforts in this space. We look forward to continuing to work with Congress on these important issues, and to answering any further questions you might have.