Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google LLC

House Committee on Oversight and Reform
Subcommittee on National Security

“Securing U.S. Election Infrastructure and Protecting Political Discourse”
May 22, 2019

Chairman Lynch, Ranking Member Hice, and members of the Committee: Thank you for inviting me to testify today about Google’s efforts to promote election integrity. I appreciate the opportunity to discuss our efforts in this space.

My name is Richard Salgado. As the Director of Law Enforcement and Information Security at Google, I work with thousands of people across teams at Google to protect the security of our networks and user data. Previously, I served as Senior Counsel in the Computer Crime and Intellectual Property Section at the Department of Justice, focusing on computer network cases involving hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other computer crimes.

Google’s mission is to organize the world’s information and make it universally accessible and useful. Efforts to undermine the integrity of democratic elections, whether by attacking election websites, promoting false information about voting stations and hours of operation, compromising candidate or campaign accounts, or otherwise, are antithetical to that mission. We remain committed to working with government, industry, and civil society to address this challenge in the United States and around the world.

To protect election integrity globally, we are building products and programs designed to detect and prevent efforts to subvert elections. In my testimony today, I will focus on four areas where we are making progress to help ensure the integrity of elections: (i) empowering people with information they can trust when going to the polls; (ii) securing elections; (iii) combating misinformation; and (iv) improving transparency of election advertisements.

Empowering People with Information They Can Trust When Going to the Polls

We created our search engine in 1998 with a mission to organize the world's information and make it universally accessible and useful. We've remained focused on this mission and the importance of providing greater access to information. This access is fundamental to helping people make sense of the world around them, exercise their own critical thinking, and make informed decisions as citizens. To this end, Google aims to make civic information more easily accessible and useful to people globally as they engage in the political process. We have been building products for over a decade that provide timely and authoritative information about elections around the world and help voters make decisions that affect their communities, their cities, their states, and their countries.

These efforts can have very practical results. In 2018, for example, we helped people in the US access authoritative information about registering to vote, locations of polling places, and the mechanics of voting. We also provided information about all US congressional candidates on the Search page in Knowledge Panels, and provided the opportunity for those candidates to make their own statements in those panels. On election day, we surfaced election results for US congressional races directly in Search in over 30 languages. We have also partnered with organizations like the Voting Information Project, with whom we've worked since 2008 to help millions of voters get access to details on where to vote, when to vote, and who will be on their ballots. This project has been a collaboration with the offices of 46 Secretaries of State to ensure that we are surfacing fresh and authoritative information to our users.

In addition to Search results about election information, we have made voting information freely available through the Google Civic Information API, which has allowed developers to create useful applications with a civic purpose. Over 400 sites have embedded tools built on the Civic Information API; these include sites of candidates, campaigns, government agencies, nonprofits, and others who encourage and make it easier for people to get to the polls.

On YouTube, to help ensure that voters could easily access authoritative content related to the candidates they were interested in ahead of the US midterm elections, we prominently surfaced information panels and the official YouTube channels for each registered congressional candidate in YouTube search results for queries related to the candidates' names.

Securing Elections

Google offers a broad array of services and tools to help campaigns, candidates and election officials reduce the likelihood of security breaches. As we saw leading up to the 2016 presidential election, the sophistication and determination of malicious actors has expanded the electoral threat landscape. We have devoted significant resources to help campaigns, candidates, and election officials improve their cybersecurity posture in light of existing and emerging threats. We strive to apply security protections automatically without requiring user intervention. When we need users themselves to take affirmative steps, we offer clear recommendations and actions.

Phishing, a fraudulent practice that tricks users into providing their account credentials, remains an ongoing threat that Google takes very seriously. Google's Safe Browsing helps protect more than four billion devices from phishing, across the web. It hunts and flags malicious extensions in the Chrome Web Store, helps block malicious ads, helps power Google Play Protect (Google's built-in malware protection for Android), and more. Safe Browsing continues to show millions of warnings about websites it considers dangerous or insecure in multiple browsers (Chrome, Firefox, Safari) and across many different platforms, including iOS and Android.

Our improving technology in this area thwarts many account hijacking efforts, including phishing campaigns, from ever reaching the inboxes of users. In addition, Google's Threat Analysis Group, a dedicated team of security professionals, further detects, prevents, and mitigates government-backed threats. Google continues to issue warnings to users when we believe they may be the targets of government-backed phishing attacks. We have issued these warnings, which include advice about ways to improve the security of users' Google accounts, since 2012.

In 2017, we unveiled the Advanced Protection Program, which provides the strongest account protection that Google offers. As part of the Program, we have conducted extensive outreach to campaigns, candidates, and election officials to promote the use of security keys, which protects users from more sophisticated and targeted phishing campaigns. The Advanced Protection Program is available to anyone, but we believe it will have particular utility for candidates, campaigns, election officials, journalists, and democracy and human rights activists.

Separately, Google and Jigsaw (an Alphabet company) have partnered on Protect Your Election, a site that provides a suite of tools to help campaigns, candidates and election-related websites protect themselves online. In addition to the Advanced Protection Program, the Protect Your Election initiative includes Project Shield, a free service that we released in 2016. Project Shield is designed to mitigate the risk of distributed denial of service attacks, which inundate sites with traffic in an effort to shut them down. These attacks can make campaign and election websites inaccessible to voters, often at critical junctures (*e.g.*, when citizens are looking for poll hours and poll location information on election day). Project Shield defends websites against attacks by filtering out and rejecting attack traffic.

We have also remained vigilant in looking for shifting strategies and techniques of attackers. Working with our partners at Jigsaw, we have multiple internal teams that work together to identify malicious actors, disable attacker accounts, secure victim accounts when necessary, and share threat information with other companies and law enforcement officials. We provide public updates about these operations. Moreover, leading up to and following the mid-term elections in 2018, we worked with companies represented in this hearing, among others, to share information in order to help detect and thwart bad actors. We also worked with the Federal Bureau of Investigation, the Department of Justice, and the Department of Homeland Security. The Department of Homeland Security was helpful in relaying information relating to state elections.

Google has supported significant outreach to increase security for candidates and campaigns across the United States and other countries. In the leadup to the 2018 election, for example, we provided trainings on email and campaign website security to over 1,000 campaign professionals and the eight major Republican and Democratic committees.

Our commitment to addressing these issues extends beyond our products, services, and engagement with government stakeholders. We've partnered with the National Cyber Security Alliance, the Congressional Cybersecurity Caucus, the House of Representatives' Chief Information Security Officer, and the Senate Sergeant at Arms to help promote better account security, including 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.

In a world where people move seamlessly between work and personal devices and accounts, it is important to assess whether current laws and rules may encumber efforts to improve the cybersecurity posture of at-risk people. We support legislation that Senators Wyden and Cotton introduced earlier this year that would explicitly authorize the Senate Sergeant at Arms, the entity responsible for securing the *work* devices and accounts of Senators and staff, to also help secure the *personal* devices and accounts of Senators and staff.

Combating Misinformation

We have a natural, long-term incentive to prevent anyone from interfering with the integrity of our products. We also recognize that it is critically important to combat misinformation in the context of democratic elections, when our users seek accurate, trusted information that will help them make critical decisions. We have worked hard to curb misinformation in our products. Our efforts include designing better ranking algorithms, implementing tougher policies against monetization of misrepresentative content, and deploying multiple teams that identify and take action against malicious actors. At the same time, we have to be mindful that our platforms reflect a broad array of sources and information and there are important free-speech considerations. There is no silver bullet, but we will continue to work to get it right, and we rely on a diverse set of tools, strategies, and transparency efforts to achieve our goals.

We make quality count in our ranking systems in order to deliver quality information, especially in contexts that are prone to rumors and the propagation of false information (such as breaking news events). The ranking algorithms we develop to that end are geared toward ensuring the usefulness of our services, as measured by user testing. The systems are not designed to rank content based on its political perspective.

Since the early days of Google and YouTube, some content creators have tried to deceive our ranking systems in order to increase their visibility, a set of practices we view as a form of spam. To prevent spam and other improper activity during elections, we have multiple internal teams that identify malicious actors wherever they originate, disable their accounts, and share threat information with other companies and law enforcement officials. We will continue to invest resources to address this issue and to work with law enforcement, Congress, and other companies.

In addition to tackling spam, we invest in trust and safety efforts and automated tools to tackle a broad set of malicious behaviors. Our policies across Google Search, Google News, YouTube, and our advertising products clearly outline behaviors that are prohibited, such as misrepresentation of one's ownership or primary purpose on Google News and our advertising products, or impersonation of other channels or individuals on YouTube. We make these rules of the road clear to users and content creators, while being mindful not to disclose so much information about our systems and policies as to make it easier for malicious actors to circumvent our defenses.

Finally, we strive to provide users with easy access to context and a diverse set of perspectives, which are key to providing users with the information they need to form their own views. Our products and services expose users to numerous links or videos from different sources in response to their searches, which maximizes exposure to diverse perspectives or viewpoints before deciding what to explore in depth. In addition, we develop many tools and features to provide additional information to users about their searches, such as knowledge or information panels in Google Search and YouTube.

Improving Transparency of Election Advertisements

Google has been working hard to make election advertising more transparent. In 2017 we committed to making improvements in this important area, and we have delivered on our commitment.

- First, we have rolled out a Verification Program for advertisers purchasing U.S. federal election ads. Each advertiser must provide government-issued identification information and other key information to confirm that the advertiser is a U.S. citizen, lawful permanent resident, or a U.S.-based organization.

- Second, to help people better understand who is paying for an election ad, we require in-ad disclosures of the name of the advertiser responsible for the election ad 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 individuals and entities buying election ads on our platforms, how much money is spent across states and congressional districts on such ads, and the top advertisers overall. The report also shows the keywords election advertisers have spent the most money on.

- Fourth, we now offer a searchable election Ad Library within our public Transparency Report which shows the election ads running on our platform and important statistics about them, including which ads had the most views, enabling deep dives into specific advertisers' campaigns.

We provide similar transparency reports for the EU Parliamentary elections and India Lok Sabha elections. Like others, we are thinking hard about elections and how we continue to support democratic processes around the world, including by bringing more transparency to election advertising online, helping connect people to useful and relevant election-related information, and working to protect election information online.

Conclusion

We appreciate that there is no panacea for the challenges that lie ahead, and we commend the Committee's efforts to ensure that we are collectively taking concrete steps to protect the integrity of our election process. Google is committed to building on our progress in the above-mentioned areas to promote the integrity of elections across the world.

Thank you for the opportunity to discuss these issues. I look forward to your questions.