Responses to Questions for the Record for Mr. Kent Walker, Senior Vice President and General Counsel, Google

Senate Select Committee on Intelligence hearing on Social Media Influence in the 2016 U.S. Elections

[From Chairman Burr]

1. What procedures must the Russian government follow to compel the production of customer-created content or personally identifiable information from your company?

We respond to Russian government requests for customer-created or personally identifiable information only pursuant to valid U.S. legal process secured through Mutual Legal Assistance Treaties (MLAT) with the United States and other diplomatic and cooperative arrangements. In extraordinary circumstances, where Google has a good faith belief that disclosure of data without delay is necessary to avert a threat to human life, Google, in consultation with an FBI legal attaché or an attorney with the Department of Justice's Computer Crime and Intellectual Property Section, may also disclose information to the Russian government. In addition, we may produce information pertaining to our Ads users who contract with our Ads business located in Russia pursuant to valid legal process in Russia and according to Russian law.

2. Has the Russian government compelled the production of customer created content or personally identifiable information from your company?

As discussed in response to Question 1 above, other than information pertaining to our Ads users who contract with our Ads business located in Russia, the Russian government may compel production of customer-related content or personally identifiable information only pursuant to valid U.S. legal process secured through an MLAT or other diplomatic and cooperative arrangements.

3. If so, has your company complied with such efforts by the Russian government to compel the production of customer-created content or personally identifiable information?

Our transparency report provides details regarding our compliance with all government requests for customer data, by country, including requests by the Russian government. The latest information is available at https://transparencyreport.google.com/user-data/overview.

4. Has your company ever refused to comply with efforts by the Russian government to compel the production of customer-created content or personally identifiable information? If so, have any of these efforts been successful?

Yes. We review each request we receive to ensure it satisfies applicable legal requirements and our policies. If we feel that a request is overbroad, we seek to narrow it. As you can see in our transparency report, available at https://transparencyreport.google.com/user-data/overview, we have not complied with every request.

5. Has your company provided any content created by a U.S. person or personally identifiable information about a U.S. person to the Russian government?

As stated in response to Question 3, our transparency report provides details regarding our compliance with all government requests for customer data, by country, including requests by the Russian government. The latest information is available at https://transparencyreport.google.com/user-data/overview.

6. More specifically, has your company provided to the Russian government the content of any direct messages sent to or from a U.S. person?

As discussed in response to Question 1 above, other than information pertaining to our Ads users who contract with our Ads business located in Russia, the Russian government may compel production of customer related content or personally identifiable information only pursuant to valid legal process secured through an MLAT or other diplomatic and cooperative arrangements. Our transparency report details our compliance with Russian government requests for customer data and is available at: https://transparencyreport.google.com/user-data/overview.

7. Has your company provided to the Russian government any information that could be used to determine the location of a U.S. person?

As discussed in response to Question 1 above, other than information pertaining to our Ads users who contract with our Ads business located in Russia, the Russian government may compel production of customer-related content or personally identifiable information only pursuant to valid legal process secured through an MLAT or other diplomatic and cooperative arrangements. Our transparency report details our compliance with Russian government requests for customer data and is available at: https://transparencyreport.google.com/user-data/overview.

[From Vice Chairman Warner]

8. Your platform allows for the continuous showing of videos to a user. Once a video is done, YouTube recommends and actually begins playing the next video based on your previous interactions. This seems particularly susceptible to foreign influence - particularly for children or young adults that use YouTube without parental supervision.

- **What are you doing to ensure the Recommendation algorithm - in the same way as the Search algorithm - is not susceptible to malign incursion?**

Google has long had numerous systems in place, both automated and manual, to detect and address manipulative and deceptive behavior across our products, including on YouTube. YouTube employs a sophisticated spam and security-breach detection system to identify anomalous behavior and malignant incursions, including attempts to inflate view counts of videos or numbers of subscribers and other similar metrics used as inputs in recommendation algorithms. In addition, while we do allow "auto-play" on You Tube, we also allow our users to control their YouTube experience. If a user does not want a new video to play after the first video has completed, he/she can turn off the "auto-play" mode with one click. Similarly, if users do not like the recommendations they are receiving, or do not want a certain video to be included as part of their history, they can delete specific videos or clear their watch history entirely.

[From Senator Collins]

9. What provisions in Google's Terms of Service ensure that political advertisements targeted toward the United States are purchased by an American citizen?

Our Terms of Service prohibit the use of our services to engage in activities that violate U.S. laws, including laws that prohibit non-U.S. persons from purchasing election ads.

10. Do your Terms of Service prohibit users from influencing elections in other countries?

Google's Terms of Service specifically prohibit activity on our platforms that violate applicable law. With respect to attempts to undermine democratic elections, we enforce policies that prohibit a range of misconduct, including content that misrepresents the owner's origin or purpose, engages in harassment, or involves posting hateful, extremist, or violent content.

We are committed to working with other governments and with Congress to strengthen protections around elections, ensure the security of users, and help combat disinformation.

11. If a foreign national working on behalf of a foreign intelligence service was an authentic user in real name on your platform, could he post divisive, but non-violent content related to a U.S. election without violating your Terms of Service? Would he be able to purchase political advertising?

Google's Terms of Service specifically require that activity on our platforms complies with U.S. law, including laws that require agents of a foreign government to label any "informational materials" they disseminate on behalf of that foreign government and laws that prohibit non-US persons from purchasing election ads. We also enforce policies that prohibit a range of misconduct by those who place content on our platforms, including content that misrepresents the uploader's origin or purpose.

[From Senator Feinstein]

12. Google has conceded that the number of people exposed to content from foreign groups online is far more pronounced through organic traffic and fake accounts than it is through paid advertising. Troublingly, it does not appear there is a proven method for combating the spread of fake accounts created to sow division in society. Although the Committee has heard testimony indicating that social media platforms have developed a number of ways to detect "bot-like" activity, as recently as August 2017, divisive foreign unpaid content designed to polarize and anger the American people could be found on social media.

- **What specific actions is Google taking to combat this type of divisive unpaid activity on an ongoing basis?**

While the majority of our platforms are not "social media", and we saw only limited use of fake accounts associated with the 2016 elections, we are deeply concerned about any attempts to use our platforms to sow division. Our systems, for example, work hard to prevent the creation of "bad" accounts by relying on a host of inputs about historical use and pattern recognition across various services. In addition, we have developed robust protections to address attempts to manipulate our systems by bots or other schemes, such as link farms. (Our webmaster guidelines provide more information about this: https://support.google.com/webmasters/answer/35769.) We use both algorithmic and manual methods, and we deploy these across our products, including Search and YouTube. We have not, however, seen the same type of social media bots as have been reported on other platforms.

We have also put significant effort into curbing misinformation on our unpaid products. That includes better ranking algorithms in Search that prioritize authoritative sources, tougher policies against the monetization of misrepresentative content by publishers. On Google News, we mark up links with labels that help users understand what they are about to read, whether it is local content, an op-ed, or an in-depth piece, and encourage them to be thoughtful about the content they view. Publishers who review third-party claims or rumors can showcase their work on Google News through fact-check labels and in Google Search through fact-check cards. We will continue to work on promoting the access to high-quality content, including partnering with the journalism industry to help people better understand and contextualize what they see online.

13. One of the more troubling findings from this investigation is the number of targeted voter disengagement efforts promoted through social media.

- **Can you say with certainty that foreign actors did not use U.S. voter registration data to target individuals through both paid and unpaid activity?**

Google did not provide U.S. voter registration data to any advertisers account.

[From Senator Cotton]

14. What type of data have you collected on Internet Research Agency actors who were using your platforms? Please be specific. Have you provided that data to law enforcement? How long is that data retained?

We have conducted an extensive review of this issue including developing a list of actors we know or suspect were involved in this effort from our research of publicly available information, the work of our security team, as well as leads we received from others in the industry, and applying those leads to nearly twenty of Google's products, including all Ads products. We have responded to the law enforcement requests regarding the information we collected as part of our review, and have and will continue to be committed to working with law enforcement and Congress to provide information relevant to their investigations, in compliance with our policies and the law.

15. Do you prevent delivery of ads to a mobile device that may be inside a polling place, where other political ads would be illegal?

We do not allow ads to be targeted to polling places.

16. Have any of Google's companies been breached by foreign actors? How many times in the last five years? What data has or could have been compromised?

Threats to our systems are continuously evolving. While we have not seen successful compromise of Google's systems in the past five years, we have encountered campaigns to gain access to the IP of companies we have acquired, and we continually address challenges from motivated and resourceful attackers. We report attacks to law enforcement and other authorities, as appropriate.

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 we recently launched our Advanced Protection Program, which integrates physical security keys to protect those at greatest risk of attack, like journalists, business leaders, and politicians. As threats evolve, we will continue to adapt to understand and prevent new attempts to misuse our platforms and will continue to expand our use of cutting-edge technology to protect our users.

17. Have you mapped the WiFi networks on military bases or in other government buildings? Do you collect information on individual Android users that may be in close proximity to, or accessing these networks?

Google's location service collects anonymous data about nearby wifi access points from Android users on an opt-in basis to improve Google's location services. We allow our users, including Governments and military bases, to opt out of that mapping by sending us a 'nomap' request as described in our help page found here: https://support.google.com/maps/answer/1725632?hl=en.

18. You have challenged the NSA for a lack of transparency and oversight, yet you collect large amounts of data and have an opaque privacy policy.

- **What types of information does Google collect?**
- **Does any non-biased third party oversee your use of personal information?**

Google is committed to protecting the privacy of our users and to providing transparency regarding the types of information we collect. In fact, *Time Magazine* and the Center for Plain Language evaluated Google's privacy policy as to be the most accessible and easy to understand of any leading technology company. See http://time.com/3986016/google-facebook-twitter-privacy-policies/. As described in our privacy policy, which you can find here: https://www.google.com/policies/privacy/, we collect information to provide better services to all of our users – from figuring out basic information about our users like which language they speak, to more complex things like which ads they will find most useful or which YouTube videos they might like. That includes information they give us and information about the services they use and how they use them. We provide users with transparency and control through easy-to-use tools that enable users to manage their privacy and security settings.

In addition to our own efforts to ensure our users can trust us with their information, Google is subject to independent, governmental oversight in the jurisdictions within which it operates, including by the Federal Trade Commission in the United States.

19. Have you ever returned revenue that was generated from advertising on webpages that facilitated Russian attempts to influence the 2016 election, terrorist propaganda, or online sex trafficking (like "backpage.com")?

Google enforces policies that prohibit a range of misconduct by those who place content on its platforms, including misrepresenting the owner's origin or purpose, engaging in harassment, or posting hateful, extremist, or violent content. We do not permit that content to be monetized on our systems. With respect to the 2016 election, the activity on our platforms was limited, with only $4700 dollars of revenue associated with ads we identified. We believe that was in large

part due to the controls we had in place prior to the election. Google and Jigsaw have recently donated considerably more funds ($750,000) to the Belfer Center for Science and International Affairs and its Defending Digital Democracy project.

20. Please provide a list of all the sources of user data that your platforms collect. Where is this data stored? How long is it retained?

As discussed in the response to Question 18, Google is committed to protecting the privacy of our users and to providing transparency regarding the types of information we collect. Our privacy policy is available here: https://www.google.com/policies/privacy/. Any data we collect is retained in accordance with our U.S. and international legal requirements.

21. According to Reuters, cyber actors linked to the Russian Government used malware implanted on Android devices to track Ukrainian artillery units. This demonstrates that Russia is not only using your platforms to influence elections, but to gain an advantage on the front lines of a battlefield.

- **How do you believe that Russia was able to accomplish this and what is being done to prevent it from occurring in the future**?

We are aware of this report and we, although with others in the industry, have questioned its accuracy. (See, e.g., https://www.voanews.com/a/cyber-firm-rewrites-part-disputed-russian-hacking-report/3781411.html). For example, that the malware at issue was not distributed through our Play Store. Regardless, as discussed in the response to Question 16, we recognize that we face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats.

22. Google processes information on various servers all over the world.

- **Is information collected on U.S. Government employees being processed or stored in countries like Russia and China?**

We do not have data centers that store information collected on U.S.-based government employees in Russia or China.

23. Has Google ever provided the governments of Russia or China access to data that it has not provided to the U.S. Government?

We respond to Russian and Chinese Government requests for customer-created or personally identifiable information only pursuant to valid U.S. legal process secured through Mutual Legal Assistance Treaties (MLATs) with the United States and other diplomatic and cooperative

arrangements. We may produce information pertaining to our Ads users who contract with our local Ads businesses pursuant to valid local legal process and according to local law. In extraordinary circumstances, we may also disclose information to the Russian and Chinese governments where Google has a good faith belief that disclosure of data without delay is necessary to avert a threat to human life, which is conducted in consultation with an FBI legal attaché or an attorney with the Department of Justice's Computer Crime and Intellectual Property Section. Our transparency report details our compliance with Russian and Chinese requests for customer data: https://transparencyreport.google.com/user-data/overview.

24. Do any Google applications or services behave differently in the United States than they do in Russia, China, or another country?

Google strives to provide our products and services in a consistent manner to our users. We may make changes to our products in certain regions based on consumer interest or legal requirements of a particular region.

25. Has Google provided information on a U.S. citizen to the government of China?

As discussed in Question 23, we respond to Chinese Government requests for U.S. customer-created or personally identifiable information only pursuant to valid U.S. legal process secured through Mutual Legal Assistance Treaties (MLATs) with the United States and other diplomatic and cooperative arrangements. Our transparency report details our compliance with Chinese requests for customer data: https://transparencyreport.google.com/user-data/overview.

26. Does Google share the personally identifiable information of its users with other countries' foreign intelligence agencies absent legal process?

As discussed in Question 23, we respond to Russian and Chinese Government requests for customer-created or personally identifiable information, only pursuant to valid legal process and vis-a-vis the U.S. Department of Justice's MLATs, with limited exceptions. Our transparency report details our compliance with these types ofrequests for customer data: https://transparencyreport.google.com/user-data/overview.

27. Is it possible that third party companies controlled by foreign intelligence agencies are purchasing personally identifiable information from Google?

No. We do not sell personally identifiable information.

[From Senator Heinrich]

28. In your testimony, you talked about finding 18 channels likely associated with Russian agents who posted 1,100 misleading and divisive videos to YouTube. These videos received 309,000 views during the election cycle.

- **What systems exist to prevent intentionally misleading or illegal content from appearing at the top of YouTube searches or YouTube video recommendations?**
- **Can the same artificial intelligence or algorithms used to police terrorist propaganda or pornography be used in this space? Why or why not?**

On YouTube, we employ a sophisticated spam and security-breach detection system to identify anomalous behavior and attempts to manipulate our systems. We remove any content that we identify on YouTube that is attempting to spam or scam our users and respond to complaints by our users. We are also working on greater transparency around news sources on our platform, including disclosure of government funding.

While some tools may work for violent extremism and terrorism-related content in a scalable way, the problem is very different for misleading or inauthentic content. Many times, the misleading content looks identical to content uploaded by genuine activists. We are dealing with difficult questions that require the balancing of free expression, 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.

29. The New York Times reported that YouTube played a crucial role in helping build and expand RT. Until recently, RT was included in Google's "preferred" news lineups, which granted them access to guaranteed revenue from premium advertisers.

- **Why did Google favor RT content?**

RT was available on YouTube's Preferred Lineup because it met our standard Preferred Lineup criteria available at: https://www.youtube.com/yt/lineups/united-states.html. Those criteria include factors such as the number of view counts of a particular channel, the number of that channel's subscribers, and the language of the channel. RT is no longer available on YouTube's Preferred Lineup.

30. What percent of Google content reviews are conducted by an actual human being rather than via automated review?

We have a global team of thousands of policy experts, reviewers, product managers, and data scientists focused on creating, maintaining, and enforcing our policies. We serve billions of

users every day, so our solutions need to work at scale. We rely on highly-trained individuals from our Trust and Safety and Security teams who work closely with machine learning tools and our algorithms to ensure our platforms are protected and there is adherence to our policies. Through a combination of sophisticated algorithms and other technologies and human review, we both proactively look for violations and respond to complaints. Technology has helped us accelerate and scale our removal process, with human review assisted by computerized classifiers and computer classifiers informed by the results of human review.

31. Are Google's content review processes the same now as they were during the 2016 election? If not, how have they changed?

We are constantly working to improve our processes and better ensure compliance with our policies. Google enforces policies that prohibit a range of misconduct by those who place content on our platforms, including misrepresenting the owner's origin or purpose, engaging in harassment, or posting hateful, extremist, or violent content.

Over the past 18 months, we have undertaken a broad effort to highlight authoritative sources and minimize the spread of misinformation on our platforms. On Google News, we mark up links with labels that help users understand what they are about to read, whether it is local content, an op-ed, or an in-depth piece, and encourage them to be thoughtful about the content they are looking at. Publishers who review third-party claims or rumors can showcase their work on Google News through fact-check labels and in Google Search through fact-check cards. To help ensure Google does not monetize content designed to mislead users, we have implemented a new policy for our AdSense publishers that explicitly bans ads on sites that misrepresent, misstate, or conceal information about the publisher, the publisher's content, or the primary purpose of the site. For Google Search, we updated our Search Quality Rater Guidelines and our evaluation test sets to help identify misleading information and unexpected offensive results, and have used this data to improve our search algorithms. This results in higher quality and more authoritative Search results.

As we announced in 2017, we are also enhancing the transparency of election ads by permitting users to find the name of any advertiser running an election ad on Search, YouTube, and the Google Display Network. We also will be releasing 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 will pair our transparency report with a publicly available repository of election ad creatives from across our Ads products.

We will continue to work on preventing the spread of misinformation by partnering with the journalism industry to help people understand what they see online and to support the creation of quality content.

32. In hiring more content reviewers, are your companies simply throwing bodies at a specific problem, or are you fundamentally rethinking how to prioritize which user interactions require additional human oversight and review. If so, how? What other changes have you made in this regard?

We agree with the suggestion that it is important to thoughtfully triage various threats to the content available on our platforms. Google was founded with a mission of organizing the world's information and making it universally accessible and useful. The abuse of the tools and platforms we build is antithetical to that mission. Google serves billions of users every day and our solutions need to work at scale. We rely not only on the thousands of human reviewers we have hired and trained, but we've also dedicated some of our top engineers to develop machine learning tools and algorithms to protect our platforms and promote adherence to our policies, focusing on key risk areas.

We face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats, but we are committed to putting our talent and technology behind addressing these problems, and will continue to build industry-leading security systems and deploy those tools in our products.

[From Senator Manchin]

33. Does Google or any Google affiliate use the information security products or services of Kaspersky Lab or any Kaspersky Lab affiliate?

Kaspersky Lab products have not been approved for use on our corporate systems. Google's policy requires that before installation of software like that offered by Kaspersky Lab, the software be reviewed by Google's security and privacy team. A review of our systems has not detected any installation of Kaspersky Lab products.

34. Does Google or any Google affiliate sell network space to RT or Sputnik news agencies?

Both RT and Sputnik do purchase ads from Google. Like all other advertisers RT and Sputnik are subject to our strict ads policies and community guidelines, including policies against advertisers misrepresenting their origin or purpose. To date, we've seen no evidence that they are violating these policies, but we continue to monitor all of our platforms to guard against potential abuse.

35. If you recently terminated any agreements with RT or Sputnik, on what date did the termination become effective?

We have not terminated any agreements with RT or Sputnik. RT was once available on You Tube's Preferred Lineup because it met our standard Preferred Lineup criteria available at: https://www.youtube.com/yt/lineups/united-states.html. Those criteria include factors such as the number of view counts of a particular channel, the number of that channel's subscribers, and the language of the channel. RT is no longer in our Preferred Lineup. That did not, however, involve the termination of any agreement with RT.

36. Do either RT or Sputnik need to purchase advertising space on your platforms, or can they freely maintain a presence or distribute web content via their own or affiliated accounts?

RT and Sputnik do not need to purchase advertising space on our platforms. Google's mission is to organise the world's information and make it universally accessible and useful. For example, on Search, we index websites such as RT and Sputnik just as we do others. We are, however, actively working to provide users and advertisers with more information about the content they are seeing to allow them to make educated choices. We have labels on Search describing RT's relationship with the Russian Government and we are working on disclosures to provide similar transparency on YouTube.

37. Does Google prohibit, or have any concern about, foreign state-sponsored news organizations posting content via any Google platform?

The aim of our content platforms, like Search and YouTube, is to bring users a diverse range of news views and opinions from across the ecosystem. Our Search results, for example, contain a variety of partly or wholly government-backed news outlets, such as BBC or France Television.

As discussed above, we are actively working to provide users and advertisers with more information about the content they are seeing to allow them to make educated choices, including whether they advertise on specific sites, such as RT. We take misinformation on our platforms very seriously, and we have put significant effort into curbing misinformation in our products. That includes a policy against news content by foreign state-sponsored news organization that conceal their affiliations with foreign governments.

[From Senator Harris]

38. Your company has produced information about Russian propaganda advertisements. Your company has also produced information about Russian propaganda that appeared as ordinary user content. You have not, however, provided information about the legitimate advertisements that accompanied Russian content.

- **How long do you retain placement and billing records for advertisements on your services?**
- **Have you instructed your relevant business units to retain the records of advertisements that accompanied Russian propaganda? If you have not, will you immediately issue that instruction?**
- **How much revenue do you estimate that you earned from the advertising that accompanied Russian propaganda?**
- **Have you notified the advertisers whose advertisements accompanied Russian propaganda?**
- **What do you plan to do with the revenue that you earned from the advertisements that accompanied Russian propaganda?**

We retain our Ads billing data and will continue to do so as is required by law, or when requested by law enforcement, and in accordance with our policies. With respect to Ads revenues associated with this effort, our extensive investigation identified very limited activity on our platforms: we identified two accounts that purchased approximately $4700 of Google ad inventory. We paid less than $35 of revenue to those actors for ads served on their published content; our earnings were a fraction of that amount. In addition, Google and Jigsaw recently donated approximately $750,000 to the Belfer Center for Science and International Affairs and its Defending Digital Democracy Project as part of our commitment to enhance the protections surrounding our democratic process.

39. The problems of inauthentic, false, and hyper-partisan content are much broader than Russian propaganda.

- **How many of the accounts on your service do you estimate are inauthentic?**
- **How much of the activity on your service do you estimate is inauthentic or false?**
- **How much of your annual revenue do you estimate is attributable to inauthentic or false content?**
- **Do you have a policy of notifying advertisers when their advertisements accompany "inauthentic or false content?**
- **What do you do with the revenue that you earn from advertisements that accompany inauthentic or false content?**

- **If you are aware of independent estimates of inauthentic or false content on your platforms, please provide those estimates. If you disagree with the estimates, please explain why.**
- **If the independent estimates were accurate, how much of your annual revenue would be attributable to inauthentic or false content?**
- **How much of the news content that is shared on your services do you estimate is false?**
- **How much of the news content that is shared on your services do you estimate is hyper-partisan?**
- **Have you conducted any studies of how false content performs on your services? If yes, please describe those studies and provide copies.**
- **Have you conducted any studies of how hyper-partisan content performs on your services? If yes, please describe those studies and provide copies.**

Google serves billions of users every day. People watch over a billion hours of YouTube content a day, we index billions of web pages on Google Search, and there are billions of emails sent each day using Gmail. It is, therefore, effectively impossible to identify every single piece of content that might be false or inauthentic. Inauthentic, false and misleading content is, however, antithetical to Google's mission, and we are committed to preventing this type of content on our platforms. Our systems rely on a host of methods to help ensure the legitimacy of accounts and content on our platforms. Those methods include:

- Assessing historical use and pattern recognition across various services in an effort to detect if an account creation or login is likely to be abusive and to prevent or detect and close "bad" accounts.
- Preventing users from creating a large number of Google Accounts in a short time period and, if we detect suspicious conduct, requiring verification.
- Curbing misinformation in our products–from better ranking algorithms that prioritize authoritative sources, to tougher policies against the monetization of misrepresentative content.
- On Google News, marking-up links with labels that help users understand what they are about to read, whether it is local content, an op-ed, or an in-depth piece, and encourage them to be thoughtful about the content they are looking at. Publishers who review third-party claims or rumors can showcase their work on Google News through fact-check labels and in Google Search through fact-check cards.
- Preventing monetization of content designed to mislead users by implementing our new policy for our AdSense publishers that explicitly bans ads on any site that misrepresents, misstates, or conceals information about the publisher, the publisher's content, or the primary purpose of the site.

- Updating our Search Quality Rater Guidelines and our evaluation test sets to help identify misleading information and unexpected offensive results, and using this data to improve our search algorithms.
- Increasing transparency for our users, including adding "nutrition labels" on Search and similar disclosures on YouTube and our recent transparency efforts around election ads.

40. In the area of state-sponsored hacking, each of your companies has a responsible senior executive and dedicated technical experts.

• Who is the senior executive responsible for countering state-sponsored information operations? When did that executive assume that responsibility, and what is the scope of the responsibility?
• As of November 2016, how many of your technical employees had the primary day-to-day task of countering state-sponsored information operations?
• As of today, how many of your technical employees have the primary day-to-day task of countering state-sponsored information operations?

Protecting our platforms from state-sponsored interference is a challenge we began tackling as a company long before the 2016 presidential election. We've dedicated significant resources to help protect our platforms from such attacks by maintaining cutting-edge defensive systems and by building advanced security tools directly into our consumer products.

We have a global team of thousands of policy experts, reviewers, product managers, and data scientists focused on creating, maintaining, and enforcing our policies and, as Senior Vice President and General Counsel of Google, leading our Legal, Policy, Trust & Safety and Philanthropy teams, I oversee many of those efforts. While the activity on our platforms associated with this effort was relatively limited — which we believe that was in large part due to the controls we had in place prior to the 2016 election — we understand the importance of maintaining and enhancing those controls as we go into the 2018 election season.

41. Much of what we now know about Russian propaganda is because of academic researchers and investigative journalists. These groups do not currently have access to the data that they need to inform the public and to build tools for detecting state-sponsored information operations. For example, these groups generally cannot assess the full set of public user activity associated with a specific topic, nor can they analyze the behavior of accounts associated with state-sponsored information operations. Providing access to this data need not come at the expense of user privacy, since these groups could be bound by non-disclosure agreements and use privacy-preserving algorithms to conduct their studies.

- **Will you commit to, by the end of the year, providing five or more independent, non-profit entities with access to the data they need to understand and counter state-sponsored information operations? If you will, please provide specifics and a timeline for bow you plan to honor the commitment. If you will not, please explain why.**

We agree that combating disinformation campaigns requires efforts from across the industry and the public sector, and we are collaborating with technology and NGO partners to research and address disinformation and, more broadly, election integrity. That includes our partnership with the Belfer Center for Science and International Affairs on its Defending Digital Democracy Project, to which Jigsaw and Google recently donated $750,000. We will continue our long-established policy of routinely sharing threat information with our peers and work with them to better protect the collective digital ecosystem. We also welcome input from law enforcement, Congress, and independent entities.

In addition, our enhancements to transparency around election ads on our platforms will include a transparency report for election ads, sharing data about who is buying election ads on our platforms and how much money is being spent and a publicly available repository of election ad creatives from across our Ads products. We will make that database available for public research to all who are interested in learning or using it to conduct research, including NGOs.

42. Similarly, much of what we now know about inauthentic, false, or hyper-partisan content is because of independent groups.

- **Will you commit to, by the end of the year, providing five or more independent, non-profit entities with access to the data they need to understand the prevalence and performance of inauthentic, false, or hyper-partisan content on your services? If you will, please provide specifics and a timeline for how you plan to honor the commitment. If you will not, please explain why.**

We take misinformation on our platforms very seriously, and we have put a lot of effort into curbing misinformation in our products, including partnering with NGOs through our trusted flagger programs, programs like the Trust Project, and our partnership with the Belfer Center for Science and International Affairs on its Defending Digital Democracy Project. We will continue to work on preventing the spread of misinformation by partnering with the journalism industry to help people understand what they see online and to support the creation of quality content. We look forward to continuing to collaborate with non-profit entities to tackle disinformation and, more broadly, election integrity.

43. Addressing state-sponsored information operations will continue to require cooperation among private sector entities and with the government.

- **Have you established a formal mechanism for promptly sharing actionable information about state-sponsored information operations with other online services, similar to the mechanisms that already exist for sharing information about state-sponsored cybersecurity threats? If not, will you commit to developing such a mechanism?**
- **The FBI is the federal agency responsible for countering foreign propaganda. Do you have a written policy of promptly sharing what you learn about state-sponsored information operations with the FBI? If not, will you commit to developing such a policy?**

We are committed to working with Congress, law enforcement, others in industry, and the NGO community to strengthen protections around elections, whether in a formal or informal setting.

44. You currently have automated systems in place to detect spam and abuse.

- **Do you have an automated system in place to detect state-sponsored information operations? If yes, will you provide this Committee with private briefing on the system's design and performance? If no, why not?**

Protecting our platforms from state-sponsored interference is a challenge we began tackling as a company long before the 2016 presidential election. We've dedicated significant resources to help protect our platforms from such attacks by maintaining cutting-edge defensive systems and by building advanced security tools directly into our consumer products. We have previously provided a detailed briefing to Committee staff on this issue and are happy to provide additional briefings as requested.

45. You have promised to adopt additional transparency and verification requirements for political advertising.

- **Please detail the new requirements and your timeline for implementing those requirements.**

Google is concerned about attempts to undermine democratic elections and we continue our ongoing efforts in this area. We have updated our advertising guidelines to prohibit ads on sites that misrepresent themselves. 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.

In addition, we have announced a number of measures to enhance transparency within election advertising:

- ***Transparency Report.*** In 2018, we'll release a transparency report for election ads, which will share data about who is buying election-related ads on our platforms and how much money is being spent.
- ***Creative Library.*** We'll also introduce a publicly accessible repository of election ads purchased on AdWords and YouTube (with information about who bought each ad). That means people will not only be able to learn more about who's buying election-related ads on our platforms, they'll be able to see the ads themselves, regardless of to whom they were shown.
- ***In-ad disclosures***. Going forward, we'll identify the names of advertisers running election-related campaigns on Search, YouTube, and the Google Display Network.
- ***Verification program.*** U.S. law restricts entities outside the United States from running election-related ads. We'll reinforce our existing protections by requiring that advertisers proactively identify who they are and where they are based before running any election-related ads. As they do, we'll verify that they are permitted to run U.S. election campaigns through our own checks.

- **How do you define the political advertisements that are covered by the new requirements? Why did you adopt the definition that you did?**

We will apply the new requirements to political advertisements that either constitute "express advocacy" or contain a reference to a clearly identified candidate, as each of those terms is defined by the Federal Election Commission.

- **Will you commit to including within your definition, at a minimum, advertisements that advocate for or against a specific candidate, political party, piece of legislation, regulatory action, or ballot referendum? If not, why not?**

As stated above, our political advertisement definition will reflect current FEC definitions of express advocacy and electioneering communications.

46. Your platform offers a range of advertisement targeting criteria.

- **Which types of targeting criteria, such as demographic, behavioral, lookalike, or email matching, did Russia use for its information operations?**

The $4,700 of ads attributable to suspected state-sponsored Russian actors were not narrowly targeted to specific groups of users: for example, we found no evidence of targeting by geography (e.g., certain states) or by users' inferred political preferences (e.g., right- or left-leaning).

47. Have you seen any evidence of state-sponsored information operations associated with American elections in 2017, including the gubernatorial elections in Virginia and New Jersey?

Protecting our platforms from state-sponsored interference is a challenge we began tackling as a company long before the 2016 presidential election. While we have not specifically detected any abuse of our platforms in connection with the 2017 state elections, our work is ongoing and we will continue to develop tools and processes to combat evolving threats.

48. User reports are an important signal of when an account is not authentic.

- **How frequently do you receive user reports about inauthentic accounts?**
- **What is your process for responding to those reports? How often does that process usually take?**
- **What proportion of those reports result in an account restriction, suspension, or removal?**
- **Among the reports that you decline to take action on, what proportion involve reported accounts that you subsequently identify as inauthentic?**
- **How many of the accounts that you have identified as associated with Russian information operations were the subject of a user report? Please provide all the user reports associated with these accounts and the actions that you took in response, including the specific time for the report and each action.**

We are unaware of any inauthentic accounts linked to Russian information operations flagged by our users. Our systems do rely on a host of inputs about historical use and pattern recognition across various services in an effort to detect if an account creation or login is likely to be abusive. The system operates to block "bad" account creation or to close groups of such accounts. We prevent users from creating a large number of Google Accounts in a short time period if our systems detect that the user might be abusive. If we detect suspicious conduct, we also require verification, aimed at detecting if a bot is attempting to access or create an account. We have also developed robust protections over the years to address attempts to manipulate our systems by bots or other schemes, like link farms. (Our webmaster guidelines provide more information about this: https://support.google.com/webmasters/answer/35769.) We use both algorithmic and manual methods, and we deploy these across our products including Search and YouTube. We have not, however, seen the same type of social media bots that have been reported on other

platforms.

49. Much of the public discussion about state-sponsored information operations on your platforms has centered on the Internet Research Agency. That is not the only group surreptitiously spreading state-sponsored propaganda.

- **What other groups are you tracking that are affiliated with the Russian government?**
- **What other countries do you believe are conducting state-sponsored information operations on your platforms? Please describe the groups that you are tracking for each country, including both government agencies and affiliates.**

The 2016 election is not the first time we have encountered state-sponsored entities trying to abuse our systems. We face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats. We will continue to build industry-leading security systems and deploy those tools in our products. Our tools will be aimed at protecting our physical and network security, but also detecting and preventing the artificial boosting of content, spam, and other attempts to manipulate our systems. As threats evolve, we will continue to adapt to understand and prevent new attempts to misuse our platforms and will continue to expand our use of cutting-edge technology to protect our users. We are happy to continue working with law enforcement and the Committee on these matters.

50. Inauthentic accounts can be disabled subsequent to automated or manual review.

- **What role do automated and human employee review play in your decision to disable a suspected inauthentic account?**
- **Do you require that a human employee review a suspected inauthentic account before it is disabled?**
- **If so, given the rate at which inauthentic accounts can be regenerated, how do you anticipate remaining ahead of the problem?**
- **What are you doing to improve automation in the process of detecting and disabling inauthentic accounts?**
- **What are you doing to make it more difficult to establish inauthentic accounts?**

Technology has helped us accelerate and scale our removal of content that violates our policies, but we also rely on highly-trained individuals from our Trust and Safety and Security teams who work closely with machine learning tools and our algorithms to ensure our platforms are protected and there is adherence to our policies. We both proactively look for violations and

respond to complaints. We take this work very seriously; in 2016 alone we removed 1.7B ads for violating policies.

As discussed in the answer to Question 48, our systems rely on a host of inputs about historical use and pattern recognition across various services in an effort to detect if an account creation or login is likely to be abusive. We have not seen the same type of social media bots that have been reported on other platforms. We understand, however, that these types of threats to our systems are continuously evolving.

51. According to news reports, Google Search and YouTube results often surface false content in response to public safety emergencies. For example, after the tragic mass shooting in Sutherland Springs, Google Search highlighted false social media content and YouTube featured false videos describing the shooter's motives. ·

- **What processes does Google have in place to identify and address false content following public safety emergencies?**
- **Has Google conducted any studies of false content following public safety emergencies? If yes, please describe those studies and provide copies. If no, will you commit to conducting such a study?**
- **Have you identified any state-sponsored information campaigns that distributed false content in response to a public safety emergency in the United States? If yes, please describe the campaigns and provide the associated content.to the Committee.**

We take misinformation on our platforms very seriously, and we have put a lot of effort into curbing misinformation in our products–from better ranking algorithms that prioritize authoritative sources, to tougher policies against the monetization of misrepresentative content. We are aware of recent issues regarding content that has appeared in the immediate aftermath of public safety events, although we have not found this material to be related to state-sponsored efforts. That said, these results should not have appeared, and we continue to make algorithmic improvements to improve the quality of our results and reduce the likelihood of this happening in the future.

Specifically regarding Google Search, we updated our Search Quality Rater Guidelines and our evaluation test sets to help identify misleading information and unexpected offensive results, and have used this data to improve our search algorithms. We regular monitor results on our products after public safety events. In the last few months, we have altered our algorithm once again to ensure irrelevant or unverified results are replaced by more relevant results.

[From Senator McCain]

52. Current campaign finance law establishes disclosure standards for television, radio, and print media. The Pew Research Center recently found that 65 percent of Americans identified an internet-based source as their leading source of information about the 2016 election.

- **Under current law, to what extent is Google responsible for providing a similar quality of disclosure to the public?**

We are committed to working with the FEC in order to enhance the transparency of digital political advertising. In a 2010 Advisory Opinion, the FEC stated that advertisers are not required to include a disclosure on the small format of AdWords because of the size of the ad or impractical nature of including additional language. (In practice, the vast majority of advertisers provide a disclosure on the landing page for the ads.) We are, however, in favor of making election advertising more transparent by implementing the following measures:

- ***Transparency Report.*** In 2018, we'll release a transparency report for election ads, which will share data about who is buying election-related ads on our platforms and how much money is being spent.
- ***Creative Library.*** We'll also introduce a publicly accessible database of election ads purchased on AdWords and YouTube (with information about who bought each ad). That means people will not only be able to learn more about who's buying election-related ads on our platforms; they'll be able to see the ads themselves, regardless of to whom they were shown.
- ***In-ad disclosures.*** Going forward, we'll identify the names of advertisers running election-related campaigns on Search, YouTube, and the Google Display Network.
- ***Verification program.*** U.S. law restricts entities outside the United States from running election-related ads. We'll reinforce our existing protections by requiring that advertisers proactively identify who they are and where they are based before running any election-related ads. As they do, we'll verify that they are permitted to run U.S. election campaigns through our own checks.

In addition to these steps, we will continue working with the FEC and Congress to promote transparency and better protect the integrity of U.S. elections.

53. In your prepared testimony, you stated that Google was committed to enhancing existing safeguards to ensure that only U.S. nationals can buy U.S. election advertisements.

- **Please describe the vetting mechanism that will be used to determine the purchaser of such advertisements.**

As discussed above, we are committed to reinforcing our existing protections and requiring increased transparency in election ads. This will include the requirement that advertisers proactively identify who they are and where they are based before running any election-related ads. We will also verify that they are permitted to run U.S. election campaigns through our own checks of FEC reporting and registration.

54. In your prepared testimony, you announced Google's intention to release in 2018 a transparency report on election advertisements.

• What information will be shared via this report?

The purpose of our report is to provide increased transparency with respect to election ads on our platforms. To that end, we plan to share data about who is buying election-related ads on our platforms and how much money is spent.

• Will the accompanying database be continuously updated for current and future elections?

Yes. We intend to update the database for current and future elections.