U.S. Senate Select Committee on Intelligence
September 18, 2024

Written Testimony
of Kent Walker
President of Global Affairs, Google & Alphabet

Chair Warner, Vice Chair Rubio, and Members of the Committee, thank you for the opportunity to appear before you today.

My name is Kent Walker, and I serve as President of Global Affairs for Google and Alphabet.

Our business relies on earning the trust of our users. And we take seriously the importance of protecting free expression and access to a range of viewpoints, while also maintaining and enforcing responsible policies.

A critical part of that responsibility is doing our part to protect the integrity of democratic processes around the world. That's why we have long invested in cutting-edge capabilities, strengthened our policies, and introduced new tools to address threats to election integrity.

We recognize the importance of enabling the people who use our services – in America and abroad – to speak freely about the political issues most important to them. At the same time, we continue to take steps to prevent the misuse of our tools and platforms, particularly attempts by foreign state actors to undermine democratic elections.

I. 2024 Election: Protecting Our Users by Disrupting Foreign Threats

This year, more than 50 national elections — including the U.S. Presidential election — are taking place around the world. With each election cycle, we apply new learnings to improve our protections against harmful content and create trustworthy experiences.

Furthering our commitment to protect elections, we created the Google Threat Intelligence group, which builds on our Threat Analysis Group, or TAG, and Mandiant Intelligence. Google Threat Intelligence helps identify, monitor, and tackle threats ranging from coordinated influence operations to cyber espionage campaigns across the Internet. TAG tracks and works to disrupt more than 270 government-backed attacker groups from more than 50 countries and publishes its findings each quarter. Mandiant similarly shares its findings on a regular basis, and has published more than 50 blogs to date this year alone analyzing threats from Russia, China, Iran, North Korea, and the criminal underground.

In the current election cycle, we have seen a variety of malicious activity, including cyber-attacks, efforts to compromise personal email accounts of high-profile political actors, and influence operations both on and off our platforms —many of which seek to sow discord among Americans. I describe some of these efforts in more detail below.

A. Combating Threats Posed by APT42

Associated with Iran's Islamic Revolutionary Guard Corps (IRGC), the group known as Advanced Persistent Threat (APT) 42 consistently targets high-profile users, including current and former government officials, political campaigns, and diplomats, as well as think tanks, NGOs, and academic institutions that contribute to foreign policy conversations. In the past six months, roughly 60 percent of APT42's known attacks have been directed against U.S. and Israeli targets, including former senior Israeli military officials and individuals affiliated with both U.S. presidential campaigns. During the 2020 U.S. presidential election cycle, we disrupted APT42 attempts to target accounts associated with the Biden and Trump presidential campaigns. These activities reflect the group's aggressive, multi-pronged effort to quickly alter its operational focus in support of Iran's shifting political and military priorities.

In the current U.S. presidential election cycle, TAG has detected and disrupted a small but steady cadence of APT42's Cluster C credential phishing activity. In May and June of 2024, APT42 targets included the personal email accounts of approximately a dozen individuals variously affiliated with President Biden or former President Trump, including current and former officials in the U.S. government and individuals associated with the two campaigns. We blocked numerous APT42 attempts to log in to personal email accounts of targeted individuals.

Recent public reporting shows that APT42 has breached accounts across multiple email providers, and we saw that the group successfully gained access to the personal Gmail account of a high-profile political consultant in June 2024. In addition to quickly securing the compromised account and sending government-backed attacker warnings to all of the targeted accounts, we proactively referred this malicious activity to law enforcement in early July, and we are continuing to cooperate with them on this matter. At the same time, we informed officials from both campaigns that we were seeing heightened malicious activity originating from foreign state actors and underscored the importance of using enhanced account security protections on personal email accounts.

TAG continues to observe unsuccessful attempts from APT42 to compromise the personal accounts of individuals affiliated with President Biden, Vice President Harris, and former President Trump, including current and former government officials and individuals associated with the campaigns.

APT42's efforts to target the U.S. presidential election are of course not limited to Google products. As documented in recent public reporting, the group has successfully breached accounts across multiple email providers and we believe this activity is ongoing. TAG has notified other service providers of this malicious activity so that they can take appropriate action on their platforms. We will continue to monitor developments and share findings with industry peers as we uncover additional activity.

B. Countering Russian-State-Controlled Influence Operations

YouTube offers many millions of channels of content and billions of videos. Since Russia invaded Ukraine, YouTube has blocked thousands of channels and millions of videos from Russian state-sponsored organizations, including channels directly tied to RT (formerly Russia Today) and Sputnik. In 2024, we terminated more than 11,000 YouTube channels linked to coordinated influence operations with ties to Russia. We also continue to terminate channels belonging to Russian entities and individuals subject to U.S. government sanctions.

Most recently, following a Department of Justice indictment issued on September 4 regarding covert Russian support to Tenet Media, and after careful review to verify violations of YouTube's Community Guidelines, we terminated Tenet Media's channel and other channels owned or operated by its owners.

Last week, the U.S. Department of State sanctioned RT for engaging in both direct disinformation and covert influence operations. These recent developments highlight the importance of receiving information from law enforcement, government, and other trusted flaggers, which add to the signals we can observe about activity on our platforms.

Finally, over the last two years, the Russian government has periodically throttled access to YouTube. In the last two months, we have seen more frequent efforts to throttle and even block YouTube in Russia. YouTube has long been one of the last remaining sources of independent media inside Russia, and has refused to comply with a number of Russian government demands to remove political speech and similar content.

C. Disrupting DRAGONBRIDGE Activity

DRAGONBRIDGE, also known as "Spamouflage Dragon," is an influence network linked to the People's Republic of China that has a presence across multiple platforms. While the majority of DRAGONBRIDGE activity remains low-quality content without a political message, a small fraction of DRAGONBRIDGE accounts post about current events with messaging that supports pro-PRC views. DRAGONBRIDGE content has also featured U.S political issues and figures, particularly in the lead-up to elections, and is often presented as short "news" clips.

In the lead-up to the 2022 U.S midterm elections, Google terminated channels in which DRAGONBRIDGE attempted to spread narratives highlighting U.S. political divisions, potential for political violence, and threats to democracy. For example, one video attempted to portray voting in the U.S. as ineffective and a waste of time. The activity extended across platforms, with DRAGONBRIDGE posting similar messages via tweets and identical video content on Twitter. In 2023, we observed pro-PRC campaigns conducting operations that targeted the upcoming 2024 U.S. presidential election. These campaigns used inauthentic accounts (positioned as coming from U.S. citizens or social movements) to promote partisan content on polarizing issues in American and global politics and to engage with U.S. voters.

In 2024 DRAGONBRIDGE continues to spread narratives highlighting U.S. political divisions and portraying the U.S. government, society, and democracy in a negative light, cycling through political and social narratives that evolve with the headlines. In May 2024, for example, DRAGONBRIDGE began uploading videos and commenting on the student protests over the Israel-Hamas war on U.S. university campuses. DRAGONBRIDGE content appeared in English, was generally pro-Palestine in its themes, and used the student protests to frame the U.S. and Western media as hypocritical.

This year, we terminated more than 22,000 YouTube channels linked to Chinese coordinated influence operations, as we publicly shared in the first quarter, second quarter, and third quarter of 2024. Though it is evident that substantial resources are being expended around pro-PRC operations, these efforts do not appear to be gaining significant traction. When we have observed them spinning up activity across platforms, we have been able to stop them relatively quickly. Google Threat Intelligence is actively monitoring DRAGONBRIDGE activity for any shifts in tone or focus related to the U.S. presidential election.

II. Securing Our High-Risk Users and Election Infrastructure

Understanding the patterns and trends of threat actors informs our approach to keeping all users and their personal information safe — and this is especially important for high-risk users during election cycles. We recommend our Advanced Protection Program — our strongest set of cyber protections — for all high-risk individuals, including elected officials, candidates, campaign workers, journalists, and election workers.

We have also expanded our longstanding partnership with Defending Digital Campaigns (DDC) to give U.S. campaigns the security tools they need to stay safe online, including tools to rapidly configure Google Workspace's security features. We encourage campaigns that are Workspace customers to enroll in Workspace for Campaigns, a free one-click feature to immediately configure 26 core security settings for an entire team. This feature is available to all campaigns eligible for support from Defending Digital Campaigns.

In 2023, through partners like DDC, we distributed 100,000 free Titan Security Keys to high-risk users. This year we have committed to providing an additional 100,000 updated versions of these security keys. Additionally our Campaign Security Project has helped train more than 9,000 campaign and election officials across the American political spectrum in digital security best practices. In the EU, we are proud to partner with PUBLIC, The International Foundation for Electoral Systems (IFES), and Deutschland sicher im Netz (DSIN) to scale account-security training and to provide security tools.

Additionally, we encourage all eligible websites supporting the election to sign up for Project Shield to increase stability during the election cycle. Project Shield helps protect against both distributed denial of service (DDoS) attacks and legitimate traffic surges, and provides free protection for websites that host information on political candidates, voting, poll monitoring, and any other websites supporting the election process.

Further, since 2014 Mandiant has provided trusted cybersecurity capacity, capability, and expertise to state and local governments through its professional and managed services. It is an active partner in CISA's Joint Cyber Defense Assistance Collaborative (JCDC) 2024 Election Cyber Defense Plan and is also supporting election security webinars for state and local U.S. election officials to help them understand their cyber threat landscape and improve their awareness of the tools and resources available to help harden election infrastructure from cyber attacks. Mandiant provides various services helping stakeholders harden and test their defenses and monitor, respond to, and recover from cyber threats, including:

- **Cyber Threat Diagnostic:** Mandiant helps customers understand their threat profile – who is targeting them, why they are being targeted, what assets the threats are targeting and how – by analyzing evidence of threat activity within their environment.
- **Exercises and Red Teaming:** Mandiant provides intelligence-informed tabletop exercises, simulations, and red teaming services to help customers validate their incident response readiness and ability to respond to real-world attacks.
- **Managed Defense and Incident Response:** Mandiant offers solutions for 24/7 overwatch and incident response expertise on-demand or on-site.
- **Proactive Threat Hunting:** Mandiant uses tailored intelligence to identify indicators of compromise as well as advanced anomalous precursors to attacks.
- **Critical Asset Protection and Attack Surface Management:** Mandiant services help customers identify their critical assets, map their entire environment, and ensure the integrity of their critical systems.
- **After-Action Reviews and Gap Identification:** After elections have concluded, Mandiant offers customers a summary of observed activities, tailored recommendations for cybersecurity improvements, and a catalog of prioritized technology gaps to remediate before the next election cycle.

III. Mitigating Risks Posed by Generative AI in the 2024 Elections

We remain on the look-out for new tactics and techniques in both cyber-security and disinformation campaigns. We are seeing some foreign state actors experimenting with generative AI to improve existing tactics, like more efficiently creating fake websites, misleading news articles, and robotic social media posts. We have not yet seen AI bring about a sea change in these tactics, but we may not always be able to see the full scope of nefarious activity, and we remain alert to new vectors of attack.

A. Empowering Users to Navigate AI-Generated Content

To combat the risks posed by AI-generated content in the context of elections, we have put in place new tools and policies and entered into partnerships with key global stakeholders.

- **AI Prohibited Use Policy:** Drawing on our experience in policy development and technical enforcement, we have created generative AI prohibited use policies outlining the types of harmful, inappropriate, misleading, or illegal content that is not allowed on our systems. We then use our extensive system of classifiers to detect and remove content that violates these policies.

- **AI Ads Disclosures:** We have long had policies against deceptively manipulated media. And last year, we were the first tech company to launch new disclosure requirements for election ads containing synthetic content. We require that federal election advertisers prominently disclose when their ads contain synthetic content that inauthentically depicts real or realistic-looking people or events. This disclosure must be clear and conspicuous, and placed in a location where users are likely to see it. This policy applies to image, video, and audio content. Ads that contain synthetic content altered or generated in such a way that is inconsequential to the claims made in the ad are exempt from these disclosure requirements. This includes editing techniques such as image resizing, cropping, color or brightening corrections, defect correction (for example, “red eye” removal), or background edits that do not create realistic depictions of actual events.

- **YouTube AI Content Labels:** We seek to give viewers relevant context about the content they watch. In mid-March, YouTube also began requiring YouTube creators to disclose when they upload realistic content – content a viewer could easily mistake for a real person, place, or event – made with altered or synthetic media, including with generative AI. We apply transparency labels to signal to users that they are watching this type of content. We apply these labels automatically for content created with certain YouTube generative AI features, like Dream Screen. For most videos, a label will appear in the expanded description, but for videos that touch on more sensitive topics — like elections, health, news, or finance — we will also show a more prominent label on the video itself.

- **Election Responsibility and Generative AI**: Last December we announced that our Gemini AI App and Search products would not provide responses for election-related prompts during the 2024 elections. As we integrate Gen AI into more consumer experiences, we are also applying election-related restrictions to many of these products, including Search AI Overviews, YouTube AI-generated summaries for Live Chat, Gems, and image generation in Gemini. Our users often use Google to get reliable and up-to-date information on topics like current candidates, voting processes, and election results — and this new technology can make mistakes as it learns or as news breaks, so we want to implement it cautiously. For many queries and prompts on Gemini, we also provide a link connecting users directly to Google Search for links to the latest and most accurate information.

- **Additional Context Features:** The About this Image feature in Search helps people assess the credibility and context of images they see online, and we recently expanded this feature to cover even more surfaces and languages where users might encounter content about which they have questions. And our double-check feature in Gemini evaluates whether there is content across the web to substantiate its responses to user prompts.

- **Digital Watermarking:** Last year we introduced SynthID, a tool that adds imperceptible watermarks to our AI-generated images and audio so that they are easier to identify. This year, we expanded SynthID to two new modalities: text and video. We are also expanding our work on identifying the provenance of AI-generated content created on other platforms through the Coalition on Content Provenance and Authenticity, as described below.

B. Working Across Industry and the U.S. Government to Address Risks Posed by GenAI in Elections

Election integrity is a shared challenge. Although we design and enforce our policies independently, we have received information for many year from national security agencies and federal, state, and local law enforcement, as well as from a range of trusted flaggers, who may have access to information and intelligence about malicious activity, including from foreign adversaries, that we do not.

Further, we have long taken a principled and responsible approach to introducing Generative AI products. And we recognize the importance of collaborating across the tech industry – including through the Tech Accord and the Coalition for Content Provenance and Authenticity – to identify emerging challenges and counter abuse.

i. Tech Accord

Earlier this year, we were proud to sign on to the Tech Accord to Combat Deceptive Use of AI in 2024 Elections, a set of commitments to deploy technology countering harmful AI-generated content meant to deceive voters. We pledged to help prevent deceptive AI-generated image, audio, or video content from interfering with this year's global elections.

As described in greater detail above and in a recent update on the Tech Accord website, we have taken a number of steps across our products to reduce the risks that intentional, undisclosed, and deceptive AI-generated imagery, audio, or video may pose to the integrity of electoral processes. We have taken steps to develop technologies, assess models, detect distribution, and appropriately address deceptive AI election content.

In line with our Tech Accord Commitments, we are also continuing our efforts to foster cross-industry resilience, provide transparency to the public, and engage with civil society. We actively share our learnings and expertise with researchers and others in the industry. These efforts include increasing public awareness by, for example, actively publishing and updating our approach to AI, our research into provenance solutions, and our approach to content labeling.

Artificial intelligence innovation raises complex questions that neither Google, nor any other single company, can answer alone. Google continues to engage and collaborate with a diverse set of partners including the Partnership on AI, ML Commons, and is a founding member of the Frontier Model Forum, an initiative to help share safety best practices and inform collective work on AI safety. We look forward to continuing to engage with stakeholders and doing our part to advance the AI ecosystem.

ii. Coalition for Content Provenance and Authenticity, or C2PA

In addition to our Tech Accord commitments, we joined the Coalition for Content Provenance and Authenticity (C2PA) as a steering committee member. The C2PA is a cross-industry effort to help provide more transparency and context regarding AI-generated content. Google has worked alongside the other members to develop and advance the technology used to attach provenance information to content.

Through the first half of the year, we collaborated on the newest version (2.1) of the technical standard, Content Credentials. This version is more secure against a wider range of tampering attacks due to stricter technical requirements for validating the history of the content's provenance, which will help ensure the data attached is not altered or misleading. We will soon bring the latest version of Content Credentials to certain key products like Search and Ads, and we will continue to expand its application to more products over time. We also encourage more services and hardware providers to adopt the C2PA's Content Credentials standard.

* * *

We are committed to doing our part to keep the digital ecosystem safe and reliable. We appreciate the Committee convening this important hearing, and we look forward to answering your questions.