Written statement of Dave Vorhaus, Google
11/8/2023
United States Senate AI Insight Forum: Elections & Democracy

Thank you to Majority Leader Schumer and Senators Young, Heinrich, and Rounds for bringing us together, and for your leadership in this critical area. Every year, voters head to the polls in the United States and many countries around the world. We have teams across the globe, working 24/7 to ensure we are prepared to support those elections. In particular, we are looking at the **role generative AI will play in elections worldwide** and the implications that has for our work. We remain committed to connecting voters to election information, helping campaigns enhance their security with the best-in-class security tools, and protecting our platforms from abuse.

Our Approach

1. Connecting voters to election information: We help voters find the information they need to participate in democratic processes. Whether someone is registering to vote for the first time, looking for their local polling place, or learning how to vote absentee, we make reliable information easily available with helpful product features that show data from trusted, nonpartisan organizations. When people search for "how to vote," they will find details about how they can vote in their state—such as ID requirements, registration, voting deadlines, and guidance for different means of voting, like in person or mail.

We work with non-partisan, third-party data partners that aggregate official data directly from state and county election administrators, and we link to the state government's official website for more information. We also support the broader election information ecosystem by offering the Google Civic Information API to make it easier for third-party developers to create useful apps to connect users with official election information.

Large Language Models (LLMs) have tremendous potential to help people learn and discover new information about the world around them. But if used incorrectly, they could also result in new information threats to elections and other world events. We have invested in tools to ensure people know when an image or video is AI generated and we have policies in place across our platforms governing manipulated media. Two important approaches that we continue to invest in to address these challenges are metadata and watermarking.

- ***Providing More Information Through Metadata.*** Metadata allows creators to associate additional context with original files, giving users who encounter an image more information.
  - Through our "About this Image" tool, Google Search users will be able to see important information such as when and where similar images may have first appeared, and where else the image has been seen online, including on news,

fact-checking and social media sites—providing users with helpful context to determine whether what they are seeing is reliable.

  - On Search, we have built information literacy features like About this Author or Page to help people evaluate the reliability of information and sources they find online. Now, we are including dedicated information literacy tools directly into the Search Generative Experience (SGE), an AI-powered feature that provides overviews and snapshots for user queries. We have introduced "About this result" in SGE, so people who have opted into Search Labs will be able to use this tool on AI-powered responses. This will give people helpful context, such as a description of how SGE generated the response, so they can understand more about the underlying technology.

- ***Strengthening Content Trustworthiness through Watermarking.*** While generative AI can unlock huge creative potential, it also presents new risks, like the spreading of false information—both intentionally and unintentionally. Google DeepMind has just launched SynthID, an experimental tool for watermarking and identifying AI-generated images. This technology embeds a digital watermark directly into the pixels of an image, making it imperceptible to the human eye, but detectable for identification. SynthID represents a significant research effort, in line with the voluntary commitments made by leading AI companies to the White House earlier this year. SynthID is being released to a limited number of Google Cloud Vertex AI customers using Imagen, one of our latest text-to-image models that uses input text to create photorealistic images.
  - While this combined approach is not infallible, our internal testing shows it is accurate—even when an image undergoes various common image manipulations. Being able to identify AI-generated content is critical to empowering people with knowledge of when they are interacting with generated media, and helping prevent the spread of misinformation.

2. Helping campaigns enhance their security: People working on campaigns and elections are higher targets for cybersecurity threats. In a 2022 study we commissioned with YouGov, 85% of high-risk professionals working in politics and journalism in the U.S. said they needed stronger cybersecurity protections, while 83% felt cyber threats against their professions had increased during the previous two years. These challenges have only grown and evolved since, especially with the spread of generative AI. We understand these concerns and are working hard to help high-risk users, such as campaigns and election officials, enhance their security with tools like our Advanced Protection Program and Titan Security Keys and educate them on how to use our products and services. We also constantly monitor and disrupt account hijackings, inauthentic activity, coordinated influence operations, and other forms of abuse on our platforms—providing quarterly updates and meeting regularly with government officials and other technology companies to share threat information around suspected election interference.

In advance of the 2024 election, we are supporting our longstanding partner Defending Digital Campaigns (DDC) in equipping campaigns with the security tools they need ahead of the U.S. 2024 elections. Through the Campaign Security Project, DDC will secure campaigns in all 50 states, providing security trainings and products at no cost. Since 2020, over the course of our partnership, DDC has secured over 380 campaigns and distributed over 20,000 Titan Security Keys, and we look forward to continuing to support DDC as we near a critical election cycle.

3. Protecting our platforms from abuse: Over the years, we have introduced new policies, enhanced our enforcement systems, and continued to invest in our teams and operations to better secure our products and prevent abuse on our platforms.

- **Policies:** We continue to make enhancements to protect the integrity of elections around the world and better secure our platforms through strict policies against elections-related abuses like voter suppression, deceptive practices, facilitating/promoting violence.
- **Threat Assessment Group (TAG)**: We have also invested heavily to counter attempts to deceive, harm, or take advantage of users, including by developing industry-leading technology to protect against spam, malware, and "content farms". Our Threat Analysis Group, which works closely with product teams like Mandiant, works to counter targeted and government-backed operations. On any given day, Google's Threat Analysis Group is tracking more than 270 targeted or government-backed attacker groups from more than 50 countries.
- **Combating Abuse with AI:** We are constantly evolving the tools, policies and techniques used to enforce our policies and protect our users. For instance, we built a prototype that leverages recent advances in LLMs to assist in enforcing our policies at scale. Using LLMs, our aim is to be able to rapidly build and train a model in a matter of days—instead of weeks or months—to find specific kinds of abuse on our products. This is especially valuable for new and emerging abuse areas; we can quickly prototype a model that is adept at finding a specific type of abuse and automatically route it to our teams for action. We're still testing these new techniques, but the prototypes have demonstrated impressive results so far and show promise for a major advance in our effort to proactively protect our users especially from new and emerging risks.
- **Political Ads Disclosure Requirement:** For years, we have provided additional levels of transparency for election ads, including "paid for by" disclosures and a publicly available ads library that provides people with more information about the election ads they see on our platforms. Given the growing prevalence of tools that produce synthetic content, later this month, we are expanding our policies a step further to require advertisers to disclose when their election ads include material that has been digitally altered or generated, including through the use of generative AI tools. This update builds on our existing transparency efforts like restrictions around who can run election-related advertising on our platform and our comprehensive political ad transparency reports. This will help further support responsible political advertising and provide voters with the information they need to make informed decisions.

Finally, when it comes to the responsibility, safety and security of high impact AI, we know we cannot do this work alone. That is why we created a $20M Digital Futures Fund through Google.org to spark more research and discussion on AI safety, security, and responsibility. In addition, together with Anthropic, Microsoft, and OpenAI, we announced our first Executive Director of the Frontier Model Forum, and the creation of a new AI Safety Fund, a more than $10 million initiative to promote research in the field of AI safety. The Frontier Model Forum, an industry body focused on ensuring safe and responsible development of frontier AI models, is also releasing its first technical working group update on red teaming to share industry expertise with a wider audience as the Forum expands the conversation about responsible AI governance approaches. We have joined the Partnership on AI (PAI) Responsible Practices for Synthetic Media: A Framework for Collective Action, as part of the community of experts dedicated to fostering responsible practices in the development, creation, and sharing of media created with generative AI.

Forums like this, the work of the Administration, and the vital input of civil society, academics, and industry bodies will enable meaningful progress, unlock more opportunity for all Americans, and ensure continued U.S. leadership. At Google, we understand that supporting elections in the U.S. and globally is a critical part of our responsibility to our users and to the democratic process. We will keep working to enhance our approach and continue these efforts next year and beyond, particularly as it relates to our commitment to being bold and responsible in promoting the acceptance, adoption and helpfulness of new high impact technologies. I am delighted to participate in this forum and answer any questions you might have about our approach. Thank you.