Leader Schumer, Senators Heinrich, Rounds, and Young,

Thank you for the opportunity to be here today. My name is Kara Frederick and I am the Director of Tech Policy at The Heritage Foundation. My research focuses on emerging technologies and their domestic and geopolitical implications. This statement is written in my personal capacity and does not necessarily reflect the views of The Heritage Foundation.

How AI Poses New Risks to Our Elections[1]

As we head into primary season for the next U.S. presidential election, the information environment is ripe for exploitation.

Advances in AI will continue to transform the information environment as computational systems become more capable of targeting information at specific users, amplifying messages, filtering information, and generating fake audio, images, and videos. AI provides mechanisms to narrowly tailor propaganda to a targeted audience, as well as increase its dissemination at scale—heightening its efficacy and reach. The advent of emerging tech could aid in an electoral campaign to do this with devastating breadth, accuracy, and scale.[2] Applications of AI with potential influence over the American democratic process include:

- **Synthetic media**
  - AI systems are capable of generating realistic-sounding synthetic voice and video recordings ("deep fakes") of individuals for whom there is a sufficient training dataset.[3] These recordings are now able to fool the untrained ear and eye.
  - Barriers to entry for deep fakes and other synthetic media are becoming lower and lower by the day—almost any enterprising individual can create their own. Their application during primary season has already begun.[4]
- **Automated spear phishing operations[5]**
- **Pattern recognition and predictions of voting trends**
  - AI systems can parse through a high volume and variety of data to provide exploitable insights into voting behaviors.
- **Highly granular voter profiling**
  - Gathering impressions, analytics, and digital personality assessments to tailor targeting attempts aimed at specific cross-sections of the voting population.
- **Tailored disinformation campaigns**

[1] Whole portions of this statement and this section in particular are drawn directly from Ms. Frederick's independently authored excerpts of the co-authored 2018 report, Artificial Intelligence and International Security, published by the Center for a New American Security during Ms. Frederick's tenure there. For more details surrounding the concepts represented in this statement, please see: https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security; "Information Security" (p.4-7) and "The Information Environment" (p.19-21).

[2] https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

[3] https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

[4] https://www.nytimes.com/2023/06/08/us/politics/desantis-deepfakes-trump-fauci.html

[5] From *Artificial Intelligence and International Security:* "AI technology offers the potential to automate this target customization, matching targeting data to the phishing message and thereby increasing the effectiveness of social engineering attacks. Moreover, AI systems with the ability to create realistic, low-cost audio and video forgeries…will expand the phishing attack space from email to other communication domains, such as phone calls and video conferencing."

    - Certain key demographics or areas can be targeted to affect voting behavior at crucial times (e.g., election night in a West Coast swing district).

- **Combining AI-driven influence operations with hard cyber hacking campaigns** at politically vulnerable moments
    - For example, this could look like an evolved version of a hacking operation in 2020, when hackers took control of an official Kuwaiti media account to actively spread falsehoods about U.S. troop presence in the region.[6] Imagine an official U.S. government account propagating AI-generated images of a fake terrorist attacks, natural disasters, martial law, etc. to shape public opinion and behavior just before an election and during voting periods.

Potential Policy Solutions[7]

Just as with most technological development, first mover advantage for AI governance is critical. Since tech development almost always outpaces attempts to govern it, the United States needs appropriate guardrails for how these technologies are built and used—guardrails imbued with American values like openness and transparency. The following recommendations can help contest the risks inherent to the use of AI in our elections, as well as their potential to advance authoritarian systems at the expense of democracies:

- **Push for appropriate transparency of AI use in political campaigns**, such as labeling and watermarks.
- **Build AI tools to detect, analyze, and disrupt disinformation** via AI-driven content identification.[8] Natural language understanding to train machines to find nefarious content using semantic text analysis could improve these initiatives.[9]
- **Promote AI explainability**, so that the behaviors of computational systems are capable of being audited. Technology should be designed in a way that accounts for the outputs it generates. Allowing for comprehensive system audits can uncover inappropriate uses of AI, such as unauthorized training of models on sensitive personal data.
- **Commit to open sourcing certain foundation models**, so potential malicious uses can be identified and resolved.[10] For example, OpenAI released elements of their large language model GPT-2 in 2019. This is good practice and could be repeated with certain foundation models. Doing so and having these changes originate within the United States and other democratic countries could help us cement our version of these technologies as superior before adversary nations like China ship and standardize their own offerings.[11]

[6] https://www.reuters.com/article/us-iraq-security-kuwait-kuna/kuwait-says-report-of-u-s-troop-withdrawal-incorrect-kuna-agency-hacked-idUSKBN1Z71LN

[7] Whole portions of this statement and this section in particular are drawn directly from Ms. Frederick's independently authored 2020 report, Democracy by Design, published by the Center for a New American Security and Ms. Frederick's 2023 FOX News article, "The US, not China, should take the lead on AI" For more details surrounding the concepts represented in this statement, please see: https://www.cnas.org/publications/reports/democracy-by-design and https://www.foxnews.com/opinion/us-not-china-should-take-lead-ai.

[8] https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

[9] https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

[10] https://www.foxnews.com/opinion/us-not-china-should-take-lead-ai

[11] https://www.foxnews.com/opinion/us-not-china-should-take-lead-ai

- **Design with privacy in mind**.[12] Tech companies should devote resources to enshrine privacy protections and transparency directly in their design. This includes tailoring investments toward data encryption, federated models of machine learning, and differential privacy—the withholding of certain forms of personally identifiable information while still sharing other, less personal data. These models consist of machine learning approaches that avoid transferring data from individual devices to a central data repository, making personal data less likely to be exploited by actors with access to that repository. Such approaches would thwart some authoritarians' ambitions of synching multiple data sources together, such as with China's social credit system, to more effectively automate control.[13]

In order to confront the new threat landscape, the United States should look to its competitive advantage: a free and open society that has been the engine of the world's innovation for multiple generations.[14] We must harness these strengths and continue to dictate the design of products the world uses. We can do this by building attractive, commercially viable alternatives to technologies developed under and beholden to undemocratic governments.[15] Technology is not neutral. Instead of generative AI services built to "uphold the core socialist values" like in China, the United States must offer and preserve democratic alternatives. Our elections, now and in the future, depend on it.

[12] https://www.cnas.org/publications/reports/democracy-by-design

[13] https://www.cnas.org/publications/reports/democracy-by-design

[14] https://www.cnas.org/publications/reports/democracy-by-design

[15] https://www.cnas.org/publications/reports/democracy-by-design