+accountabletech

July 31, 2023

Dear Dr. Greene, Dr. Tao and other members of the PCAST Working Group on Generative AI:

Thank you for the opportunity to share input with the Presidential Council of Advisors on Science and Technology regarding generative AI, and on how best to mitigate its risks.

This comment is submitted by Accountable Tech, a nonpartisan, nonprofit organization that advocates for structural reforms to repair our information ecosystem and foster a healthier and more equitable democracy. This comment pertains most directly to questions 1, 2, and 4 of your request for public input.

We applaud the Biden administration for its leadership – most recently in bringing the largest AI companies together around a set of basic voluntary safeguards – as global policymakers race to curb the dangers of AI. Voluntary private sector commitments related to independent security testing, watermarks to identify AI-generated content, more transparent public reporting, and increased risk-research are important first steps.

But let's be clear: lowest-common-denominator voluntary safeguards are no substitute for comprehensive executive and legislative action.

As Accountable Tech recently outlined in our public comment to the White House Office of Science and Technology Policy, there are myriad accountability measures the administration can and must deploy in the short-term, which are relevant to the Presidential Council of Advisors on Science and Technology's request for input – along with additional priorities to focus on – including:

Vigorously enforce the breadth of pertinent laws already on the books.
When it comes to addressing many of the concerns related to civic engagement outlined in the President's Council of Advisors on Science and Technology's request for public input, it's important to note that there is no AI exemption from federal laws and statutes when generative AI tools are leveraged to unlawfully manipulate our elections, including:

- *Schemes to deprive individuals of their right to vote freely*. There are numerous federal statutes that make it unlawful to interfere with an individual's right to vote, including Section 131(b) of the Civil Rights Act of 1957, Section 11(b) of the Voting Rights Act of 1965, and Section 2 of Ku Klux Klan Act, which makes it a federal crime for two or more persons to conspire to "injure, oppress, threaten, or intimidate any person... in the free exercise or enjoyment of" the right to vote. These laws apply to online behavior just as offline. For example, a federal jury recently convicted a man who conspired with others using social media to target thousands of individuals with fraudulent messages about how to cast their ballots in an effort to deprive them of their right to vote. Generative AI could turbocharge online voter suppression and intimidation by empowering people to easily execute such schemes with greater scale and sophistication, and via other means, like the generation of images or videos that fraudulently depict threats or irregularities at voting sites. In some cases, the developer of an AI system might even have liability, like if they built a chatbot marketed as a newfangled search engine that was found to be widely distributing false voting information.

- *Foreign election interference*. Generative AI also threatens to unleash a flood of unlawful election influence operations, making it infinitely easier, for example, for malign foreign actors and their agents to manufacture compelling propaganda at scale and target it at susceptible voters to boost their preferred candidate. Although there are large loopholes in existing laws like the Foreign Agents Registration Act (FARA) and the Federal Election Campaign Act (FECA), the federal government should enforce these statutes aggressively and level appropriate sanctions to deter foreign election interference.

Utilize the full scope of executive authority to curtail AI-related harms, including the FTC's commercial surveillance rulemaking process to establish new bright-line limits on unfair and deceptive data practices. Among other things, the administration should consider moving to:

- *Prohibit surveillance advertising and/or other secondary data uses*. Accountable Tech submitted a lengthy rulemaking petition in 2021 urging the FTC to prohibit surveillance advertising – a toxic business model that drives sweeping harms to consumers, the information ecosystem, and society and democracy writ-large – as an unfair method of competition. This is all the more urgent in the context of generative AI, as voters could soon be served personalized political ads that have been uniquely generated to exploit their specific vulnerabilities and interests based on Big Tech's extensive tracking and profiling. In a compelling submission on that petition docket, Consumer Reports and EPIC outlined several other approaches the FTC could take to promulgate rules prohibiting secondary uses of data that constitute unfair or deceptive acts or practices, any of which would offer significant new protections to voters online and mitigate the harms of generative AI.

- *Issue an executive order implementing the Blueprint for an AI Bill of Rights, as proposed by the Center for American Progress*. The White House could build upon their estimable work on the Blueprint for an AI Bill of Rights by having President Biden issue an executive order that would effectively require its implementation across all federal agencies for their own procurement and deployment of AI systems, in addition to other mechanisms to encourage its adoption and incentivize investments in responsible AI more broadly.

Leverage the bully pulpit to catalyze efforts to clarify rules related to generative AI, including clarifying that bans on "fraudulent misrepresentation" in political ads applies to AI-generated deepfake videos, and that Section 230 immunity does not apply to generative AI companies.

- *Clarify that bans against "fraudulent misrepresentation" in political ads also applies to AI-generated deepfake images and videos, as proposed by Public Citizen*. With candidates for federal office and their agents already weaponizing deepfakes for political gain, and rapid technological advances empowering increasingly realistic misrepresentations, it is critical that the FEC issue a new rule or guidance – or at least consider public comments on the issue – clarifying that intentional misrepresentations of candidates or political parties in campaign ads is unlawful under the FEC Act. Amidst multiple petitions for rulemaking that would do just that from advocacy group Public Citizen, the FEC blocked the agency from hearing public comment. In response, 50 lawmakers submitted their own request, saying that "as the 2024 Presidential election quickly approaches, it is imperative that the FEC allow comment on Public Citizen's petition for rulemaking." Although deep regulatory and jurisdictional questions remain, the Biden Administration should use the power of the bully pulpit to urge the FEC to hear public comment and further explore feasible options for limiting the use of deepfakes in political advertising.

- *Clarify that Section 230 does not apply to generative AI, as outlined in the "No Section 230 Immunity for AI Act*." A critical step to ensuring more responsible use of AI technology is to clarify that generative AI companies are not granted immunity under Section 230. Clarifying that immunity does not extend to generative AI companies will create a better incentive structure for generative AI companies to place stricter limits on the creation and deployment of generative deepfake images and videos, and put more power in the hands of individuals to defend themselves in the court of law in the case of defamatory or otherwise harmful uses of deepfake technology.

Coordinate cross-sector efforts to develop effective and interoperable standards for watermarking and content verification. As the Biden Administration has already made clear, watermarking AI-generated or substantially manipulated videos, images, and audio to identify the provenance and authenticity of content in metadata and/or disclosure labels is a critical first step that can add key context that helps protect both consumers and creators of content. Here, the administration should specifically work to persuade leaders across all relevant industries – including AI developers, online platforms, and publishers – to embrace unified and interoperable technical standards to ensure efficacy, like what has already been started by groups like C2PA. And the White House should also immediately commission studies to evaluate the benefits and drawbacks of various approaches to watermarking across different content mediums, as more research is urgently needed to inform standard setting in this space.

Further, there should be bright-line prohibitions on certain unacceptable uses, such as non-consensual dissemination of deepfake sexual images; willfully deceiving a person with the intent of impeding their exercise of the right to vote; or impersonating someone and acting in their assumed character with the intent of obtaining a benefit or injuring or defrauding others. Related, it is also worth exploring additional measures to verify official government messages, systems, alerts, and communications to ensure authoritative, accurate, trusted, and effective communications between citizens and their government officials and representatives.

As demonstrated throughout this comment, the administration has compelling tools at its disposal to confront the urgent threats large-scale AI systems pose to our elections and democracy. We urge the Biden Administration to take further, immediate action to curtail AI-related harms by: keenly enforcing federal statutes already on the books against voter suppression and foreign election interference; using the full scope of its authority and bully pulpit to clarify that deceptive AI ads violate FEC's prohibition on fraudulent misrepresentation; clarifying that Section 230 should not extend to generative AI companies; the FTC's commercial surveillance rulemaking process; and continuing to prioritize a cross-sector system for effective and interoperable watermarking.

Accountable Tech is eager to work with a wide range of public and private stakeholders to develop structural reforms to address these threats in the short-term before it’s too late. The 2024 elections are just around the corner, and it is imperative that the United States takes urgent and immediate action to prepare for the challenges to come. We stand ready to collaborate on the road ahead and continue our efforts to protect democracy and strengthen our information ecosystem.