+accountabletech

July 7, 2023

Dr. Arati Prabhakar
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Director Prabhakar,

Thank you for the opportunity to respond to the White House Office of Science and Technology Policy's Request for Information (RFI) regarding national priorities for artificial intelligence (AI).

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 to questions 1, 7, 10, 11, 14, 15, 16, 26, and 29 in OSTP's request for comment.

The potential economic and social benefits of AI-powered technologies – along with the hype cycle surrounding it – have understandably generated a swell of excitement. Unfortunately, the current trajectory of the AI arms race has us far away from realizing those rosy visions, and instead demands we grapple with the urgent threats these systems are exacerbating.

Accountable Tech has spent years working to address the systemic drivers of the information crisis we are living in, which has pushed democracy to the brink – from campaigning to end the surveillance advertising business model that rewards harmful lies and extremist content, to devising a sweeping election integrity roadmap to combat efforts to deceive voters and manipulate public discourse.

The arrival of generative AI adds harrowing new layers to the ever-deepening information crisis. Generative AI tools are capable of producing fake news articles, social media posts, videos, and audio clips that are becoming less and less distinguishable from authentic content. These tools are widely accessible today and are already being used to wage coordinated propaganda campaigns that threaten to undermine elections and democratic institutions, posing an immediate and urgent threat.

We applaud the Biden administration for the steps it has already taken to harness the good and confront the harms of AI writ-large – from engaging key stakeholders, to hosting learning sessions, and releasing an AI Bill of Rights,[1] among many other efforts – and for issuing this RFI to solicit input from public interest groups like Accountable Tech and other stakeholders as that critical work continues.

We have been pleased to have the opportunity to weigh in on important AI-related issues from various perspectives, including through our recent submission regarding the cloud computing

[1] https://www.whitehouse.gov/ostp/ai-bill-of-rights/

market and comments on the ongoing merger guideline review and the FTC's commercial surveillance rulemaking. And in forthcoming work, we will outline a bold and holistic approach for grappling with the full range of AI harms. But for the purposes of this RFI, we will focus narrowly on urgent steps the Biden Administration can take to address the immediate threats new generative AI systems pose to the integrity of our elections and democracy.

I. <u>SUMMARY OF HARMS</u>

There is no shortage of literature underscoring the breadth and severity of the harms emanating from generative AI – including the potential for increased bias and discrimination, further erosion of individual rights and privacy, and exploitation of artists, journalists and content creators. For a deeper exploration of these threats, we would point to reports recently released by our friends at EPIC,[2] Public Citizen,[3] and the Norwegian Consumer Council.[4]

However, we believe there is no more immediate threat among these to U.S. interests and democratic values than the capacity for generative AI to further erode the information ecosystem and public discourse, manipulate elections, and undermine faith in institutions at scale.

Currently available tools like ChatGPT, DALL-E, and Midjourney are capable of generating election-related content that could radically shift public opinion and public trust in elections.[5] As the *Associated Press'* David Klepper notes, these tools are capable of easily making "automated robocall messages, in a candidate's voice, instructing voters to cast ballots on the wrong date; audio recordings of a candidate supposedly confessing to a crime or expressing racist views; video footage showing someone giving a speech or interview they never gave[; and] fake images designed to look like local news reports, falsely claiming a candidate dropped out of the race."[6]

Once generated, this kind of false content can spread like wildfire – either organically, through algorithmic recommendation, or via bad actors manipulating paid and organic features for reach. The potential impacts are alarming: disinformation campaigns can isolate marginalized communities, suppress voter turnout, and dramatically alter election results.

Threats of this kind are far from hypothetical. This spring, a Twitter account designed to look like an authoritative Chicago news outlet published a widely circulated AI-generated deep fake video of a mayoral candidate espousing an unpopular opinion on police reform the night before the election.[7] Ron DeSantis' presidential campaign shared realistic AI-generated images of former President Donald Trump hugging Anthony Fauci to falsely discredit his rival.[8] And on May 22, an AI-generated image depicting an apparent explosion at the Pentagon was picked up by U.S. and international media outlets and quickly caused investor panic with the S&P 500 dropping and U.S. Treasury bonds and gold prices rising.[9] Although not election-related in this context, it's an example of how AI-generated content can lead to real-world harm and could also be used to manipulate voters on or around Election Day.

[2] https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf
[3] https://www.citizen.org/article/sorry-in-advance-generative-ai-artificial-intellligence-chatgpt-report/
[4] https://storage02.forbrukerradet.no/media/2023/06/generative-ai-rapport-2023.pdf
[5] https://www.safe.ai/ai-risk#Misinformation
[6] https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election
[7] https://www.cbsnews.com/chicago/news/vallas-campaign-deepfake-video/
[8] https://www.nytimes.com/2023/06/08/us/politics/desantis-deepfakes-trump-fauci.html
[9] https://apnews.com/article/pentagon-explosion-misinformation-stock-market-ai-96f534c790872fde67012ee81b5ed6a4

With thousands of electoral campaigns kicking off in the run-up to 2024 – coupled with the wide accessibility of AI tools here and now – events like these are only going to become more frequent. Even industry leaders are acknowledging the severity of the threat, with OpenAI CEO Sam Altman recently testifying that he is particularly concerned with AI's ability "to manipulate, to persuade, to provide sort of one-on-one interactive disinformation" in relation to elections.[10]

II. THE NEED FOR SWIFT ACTION

If the rise of today's tech giants teaches us anything, it is the failure of self-regulation – a case-study in what happens when an industry committed to moving fast and breaking things is met with years of inaction from the policymakers tasked with holding them accountable. With a litany of AI-related harms already being felt, and advancing as fast as the technology itself, we cannot afford to repeat the costly mistakes of the social media era.

We should be skeptical of a call for overly slow and deliberative action; many of those calls are coming from the industry itself, which stands to gain from circumspect government action.[11] For example, Kent Walker, Google's president of global affairs, recently offered praise for legislative proposals that begin with long-information gathering processes, saying, "Sometimes it's not terrible to be a little incremental — to see exactly how it's developing in society, what risks are manifesting and what benefits are out there, and how do we tweak and adjust."[12]

Microsoft's chief economist Michael Schwarz went as far as to explicitly argue that "we shouldn't regulate AI until we see some meaningful harm that is actually happening," noting that "the first time we started requiring driver's licenses, it was after many dozens of people died in car accidents, right? And that was the right thing."[13]

With the scale of potential harm from generative AI, we cannot afford to wait. Yes, we will need to tweak and adjust our policies as technology changes, but that shouldn't keep us from putting common sense rules of the road in place now. Many industry leaders may appear to be eager for regulation, but as we point out in Fast Company, they have played a PR game before: voicing concern and asking Congress to pass legislation while talking out the other side of their mouth and spending millions to defeat the very legislation they publicly praise.[14]

One argument they've used: We need time to find the silver bullet solution. But the truth is, no silver bullet exists and we don't have time to waste. Urgent action is needed to put a check on some of the worst potential harms – and steer the best uses – of AI.

This is not a moment to let the perfect be the enemy of the good. There are meaningful and viable interventions to curb some of the worst immediate disinformation harms of AI, as we elaborate below. As global democracies grapple with emerging technologies, we also stand to benefit from global coordination.

A year ago, most non-technologists couldn't have imagined generative AI being in the place it is today. While we cannot elucidate the scary potential of generative AI to deceive voters a year from now, we're already seeing examples of AI content in electioneering today.[15] The truth is we

[10] https://www.washingtonpost.com/technology/2023/05/16/ai-congressional-hearing-chatgpt-sam-altman/
[11] https://www.washingtonpost.com/politics/2023/06/13/google-bucks-calls-new-ai-regulator/
[12] https://subscriber.politicopro.com/newsletter/2023/06/google-weighs-in-on-washingtons-ai-plans-00103240
[13] https://arstechnica.com/tech-policy/2023/05/meaningful-harm-from-ai-necessary-before-regulation-says-microsoft-exec/
[14] https://www.fastcompany.com/90896781/openai-ceo-sam-altman-the-new-mark-zuckerberg
[15] https://www.nytimes.com/2023/06/25/technology/ai-elections-disinformation-guardrails.html

cannot predict how the technology will take root in absence of regulation, nor in a meaningful way with it, but that cannot be a reason to abdicate responsibility.

Industry leaders have deployed numerous tactics to cast themselves as thoughtful while delaying accountability. They've played up the long-term threat of human extinction, asked Congress to create a new agency, and heaped praise on proposals that would slow-walk action – all while continuing to drive the AI arms race forward at a breakneck speed. But concrete harms from these systems are already being felt, and advancing as rapidly as AI itself. As officials across federal enforcement agencies have underscored, there is no AI exemption from the laws on the books; enforcing them swiftly and vigorously is a critical first step toward mitigating automated harms and deterring the reckless deployment of unsafe systems.

III. URGENT ACTIONS THE ADMINISTRATION SHOULD PRIORITIZE

In forthcoming work, Accountable Tech will outline a comprehensive AI accountability platform addressing the full range of AI harms and underlying drivers, including the need for Congress to finally pass robust federal privacy legislation and updated antitrust laws with bright-line rules and strong enforcement mechanisms. But given the urgency of addressing immediate harms to the information ecosystem and democracy, and the scope of this Request For Information, this comment focuses on levers the Biden Administration can pull without waiting for Congress to act.

Vigorously enforce the breadth of pertinent laws already on the books. Leaders of key agencies have already made clear that there is no AI exemption from federal laws that "protect civil rights, fair competition, consumer protection, and equal opportunity."[16] And there are countless ways the developers and deployers of advanced AI systems are already violating these laws – from automating discrimination in housing[17] and lending,[18] to AI-related abuses of children's data[19] and unfair or deceptive practices.[20] Similarly, although regulators have a limited toolkit in the fight against AI-related threats to our democracy, they must aggressively enforce existing federal 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.[21] 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

[16] https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf

[17] https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known#:~:text=Settlement%20Agreement,-These%20are%20the&text=Meta%20has%20until%20December%202022,algorithms%20actually%20deliver%20the%20ads.

[18] https://www.cnbc.com/2023/06/23/ai-has-a-discrimination-problem-in-banking-that-can-be-devastating.html

[19] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever

[20] https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust

[21] https://www.brennancenter.org/our-work/research-reports/federal-laws-protecting-against-intimidation-voters-and-election-workers

how to cast their ballots in an effort to deprive them of their right to vote.[22] 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 by leveraging the ongoing merger guideline review to embolden enforcers to more robustly confront unfair methods of competition, and 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.[23] 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,[24] 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.*[25] 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.

- *Clarify that deliberately deceptive AI campaign ads violate the FEC's prohibition on fraudulent misrepresentation, as proposed by Public Citizen.*[26] With candidates for

[22] https://www.justice.gov/usao-edny/pr/social-media-influencer-douglass-mackey-convicted-election-interference-2016

[23] https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf

[24] https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf

[25] https://www.americanprogress.org/article/the-needed-executive-actions-to-address-the-challenges-of-artificial-intelligence/

[26] https://www.citizen.org/article/petition-for-rulemaking-to-clarify-that-the-law-against-fraudulent-misrepresentation-applies-to-deceptive-ai-campaign-ads/

federal office and their agents already weaponizing deepfakes for political gain, and rapid technological advances empowering increasingly realistic misrepresentations, the FEC could mitigate these threats by issuing a new rule or guidance clarifying that intentional misrepresentations of candidates or political parties in campaign ads is unlawful under the FEC Act.

Leverage the bully pulpit to advance AI accountability, including encouraging industry leaders to collectively embrace key standards, supporting plaintiffs seeking redress from AI harms, and pressuring Congress to swiftly pass important bipartisan legislation. On each front, the backdrop of the EU racing to finish[27] its AI Act[28] – which could soon saddle companies with new obligations and once again leave Congress on the sidelines as Brussels rewrites the rules of the digital world – should provide the White House with additional points of leverage. Below are specific examples of worthwhile endeavors in each of those domains:

- *Industry.* In line with the principles outlined in the AI Bill of Rights and the NIST Risk Management Framework, the administration should push industry leaders to commit to key transparency and accountability standards that would open up black box automated systems and equip users with critical context to avoid manipulation. Concurrently, the administration should launch studies to determine best practices for each mechanism, including:
    - *Datasheets*[29] comprehensively documenting the datasets upon which models were trained and evaluated.
    - *Model cards*[30] or *system cards*[31] outlining intended uses, caveats, and safeguards; the main parameters that determine a model's behavior; and how users will be notified they are interacting with AI-generated or -manipulated content.
    - *Watermarking* all AI-generated or substantially manipulated videos, images, and audio to identify the provenance of content in metadata and disclosure labels where appropriate. 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 (see efforts from the nascent C2PA[32]) to ensure efficacy.
    - *Pre-deployment systemic risk assessments* and mitigation with public reporting, and annual *post-deployment impact assessments* with independent, third-party auditing and disclosure.
- *The Courts.* The administration should seek opportunities to file amicus briefs and statements of interest in cases that will shape the future of accountability for AI-related harms – in particular to clarify that developers and deployers of generative AI systems are not broadly shielded from liability by Section 230. Defamation cases targeting ChatGPT are already unfolding;[33] with chatbots persuading individuals to take their own

[27] https://www.euractiv.com/section/artificial-intelligence/news/ai-act-enters-final-phase-of-eu-legislative-process/
[28] https://artificialintelligenceact.eu/
[29] https://arxiv.org/pdf/1803.09010.pdf
[30] https://arxiv.org/pdf/1810.03993.pdf
[31] https://montrealethics.ai/system-cards-for-ai-based-decision-making-for-public-policy/
[32] https://c2pa.org/
[33] https://news.bloomberglaw.com/ip-law/first-chatgpt-defamation-lawsuit-to-test-ais-legal-liability

lives[34] and advising people with eating disorders to pursue extreme weight-loss,[35] more serious cases will surely follow. Establishing precedent about the limits of Section 230 protections via clear-cut cases in which generative AI tools have inflicted severe and easily foreseeable harms can fundamentally change the calculus for those who have been developing and hastily deploying these high-risk systems with impunity.

- *Congress.* Despite all the well-founded frustration over US lawmaker's long-running failure to forge any progress on tech accountability issues, the reality is that historic legislation on both privacy[36] and competition[37] advanced through key committees last Congress with overwhelming bipartisan support, thwarted only by not being brought to the floor. Both the American Data Privacy and Protection and Privacy Act (ADPPA) – with its data minimization requirements and strong civil rights protections – and the sweeping Big Tech antitrust package would go a long way toward addressing systemic AI harms. Rather than starting from scratch and trying to forge consensus on controversial new AI measures, the White House should use its political capital to swiftly drive forward the strongest possible versions of those bipartisan bills and sign them into law.

IV. CONCLUSION

As demonstrated throughout this comment, the administration has ample tools at its disposal to confront the urgent threats large-scale AI systems pose to our elections and democracy. Now, it must deploy them swiftly and strategically to deter catastrophic societal harms. If we fail to take adequate action in the coming months, we may well be paying the price for decades.

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.

[34] https://www.businessinsider.com/widow-accuses-ai-chatbot-reason-husband-kill-himself-2023-4

[35] https://www.vice.com/en/article/qjvk97/eating-disorder-helpline-disables-chatbot-for-harmful-responses-after-firing-human-staff

[36] https://thehill.com/policy/technology/3567822-house-panel-advances-landmark-federal-data-privacy-bill/

[37] https://www.cnn.com/2021/06/24/tech/house-judiciary-markup-big-tech-breakup-antitrust-bill/index.html