

The State of Generative AI in the 2024 Election Year

In January 2024, voters in New Hampshire received robocalls that sounded like President Biden telling them not to vote in the state's primary election. The calls were fake and made with AI technology. This marked one of the first documented cases of generative AI being used to suppress voter turnout in American elections. Similar AI tactics emerged during Slovakia's elections, where fake audio recordings attempted to influence voters just days before the election. These incidents highlight how AI has become a major concern for election security in 2024.

While there is general consensus that AI technology will play a significant role in how voters navigate the election landscape, researchers and activists find themselves at odds on what this means for the impact of AI within elections and how to proceed. This brief examines two different viewpoints from research organization The Brookings Institute, who focus on public policy research and analysis, and civil rights organization The Leadership Conference, who focus on advancing civil and human rights for all Americans. While Brookings advocates for a measured approach that balances the benefits and risks of AI, The Leadership Conference argues that AI primarily threatens minority communities and civil rights protections.

Regulatory Code: AI, Civil Rights, and the Future of Our Democracy

Hosted by The Leadership Conference

Concerns regarding misinformation, legal regulation, and bias built into the training of these AI have been topics of important discussion with the growth of generative AI. Civil rights organizations are highlighting the needed urgency in addressing AI's role in shaping political discourse and decision making. Here's an overview of what various leaders have to say about how to ensure the ethical use of AI demands intentional scrutiny to preserve fairness and transparency in our electoral process.

Generative AI has introduced a new landscape in how information is disseminated and consumed by the public. While this has a lot of benefits for the elections process, it also presents many unique challenges that disproportionately impact minority communities. It has already been key in creating sophisticated misinformation campaigns that target minorities. For non-english speaking communities, this impact can be significantly amplified by lack of proper monitoring and detection of misinformation on non-English channels. There is also a high reliance on social media platforms such as TikTok for news and information in these communities, where regulation is less formal compared to traditional media channels, putting them at an even more vulnerable position. Without proper mechanisms to monitor, detect, and remove misinformation in non-English languages, these

communities will continue to be at a higher risk of AI directed misinformation.

This risk of misinformation is continually amplified by the fact that many AI training datasets have built in historical biases, which can lead to bias in the resulting output when using these AI systems. This can be particularly concerning in the context of elections. This issue is bigger than the idea of deep fakes or robo calls - it can permeate systems such as signature match verification efforts for mail in ballots, in which Asian surnames are rejected at a higher rate than other surnames. Even the barrier of entry for acts such as cyber attacks are lower; people can create a variety of nuisance requests to target local elections, and you no longer need to be a well versed programmer to do so.

Social media platforms play a pivotal role in this ecosystem, and can hold the power to shape what the conversation about these issues looks like. The approach by social media platforms to handle the spread of AI generated misinformation will be critical as we approach the 2024 election. While there are rules and regulations being developed by these AI companies, they have not yet been tested. It's important to remember that the social media companies that we would like to put these regulations in place are the same companies producing these AI, from Bard by Google, Chat GPT by Open AI & Microsoft, Meta AI by Meta. These organizations should have civil rights infrastructure built into everything they do, so that all of their products can be built from a civil rights perspective.

There are potential solutions in the works. To start, we should encourage companies to hold themselves accountable. It is hopeful that Congress will take action as there is generally bi-partisan support on this issue - five states have already passed legislation to ban deep fakes used in elections. Most importantly, we need to continue investing money into organizations that are already doing this civil rights work. It is important to get resources out now, and to inform voters of these new threats so that they know how to act and how to participate in a democracy while navigating the impacts of AI.

Assessing the impact of generative AI and other online threats in a historic election year

Hosted by The Brookings Institute

The Brookings Institute hosted a panel bringing together the brightest minds around Generative AI and the potential threats it brings during a historic election year, what we can do to combat it, and how they see the threat evolving in the future. Some of the biggest takeaways from the panel are summarized below:

The good news is that much of this technology is still not perfect. Even with a ton of money poured into it, AI is still not able to generate super believable deep fakes that will fool the masses. Because of this, the public is starting to catch on to the deepfake antics, and just like how photoshop used to fool people, the public will adapt. However, the bad news is that

there are very few studies on the impact these deep fakes have. It's really difficult to quantify their impact and so very few credible studies have been done looking into it.

When tackling the issue of deep fakes, we need to be content agnostic. It is not about what they are sharing, but rather who is sharing the deep fakes; this will allow us to be able to identify and take down the bad actors. Empowering people with the education they need to understand and spot deep fakes is the best way for us to tackle the generative AI issue. Take away the bad actor's power to fool anyone, and the issue becomes less severe.

So how will this threat evolve in the future? Everybody is talking about this threat and assessing how to tackle it. It is getting attention from Data Scientists and Data Analysts who are working on ways to deal with generative AI and educate people on its uses. The U.S. Government is taking this threat seriously, and looking to track down and punish bad actors to combat the people in charge of creating these deep fakes. People working in campaigns are used to dealing with threats like this every year. The threat may evolve or change, but there are always those looking to interfere with elections. There are also already federal laws in place making it illegal to deceive voters, and creating generative AI deep fakes will likely fall under those laws.

Overall, we are not empty-handed in combating the generative AI deep fake threat. People across the country are working in this space already to tackle these issues as they pop up, and with education, funding of investigative journalism, and lawmakers working against the bad actors, the panel believes this threat will come and go like any of the others that have come before it.