BRENNAN CENTER FOR JUSTICE

June 4, 2024
California Senate Elections and Constitutional Amendments Committee
California Assembly Elections Committee
Joint Hearing
"Artificial Intelligence and Elections: Protecting Democracy in the Digital Era"
Testimony of Liz Howard, Brennan Center for Justice

Chair Blakespear, Chair Pellerin and Members of the Committee on Elections and Constitutional Amendments and the Committee on Elections:

Thank you for the opportunity to testify at this important hearing, *Artificial Intelligence and Elections: Protecting Democracy in the Digital Era*. For over a decade, I have worked with election officials on election administration issues. In my former position as deputy commissioner of elections in Virginia, I led various election security projects, including the decertification of all paperless voting machines in the commonwealth. In my current role, I work closely with state and local election officials across the country on election administration issues, including election security. I have also co-authored multiple reports on election security and policies that will better enable our election infrastructure to withstand attacks and keep our elections – and election officials – safe, including *How Election Officials Can Identify, Prepare for, and Respond to AI Threats*.

The Brennan Center for Justice — a nonpartisan law and policy institute that focuses on democracy and justice — appreciates the opportunity to share our work with election officials related to the threats that artificial intelligence poses to election administration and ways to protect against these threats.[1] The election officials in California and around the country who are busy preparing for a safe and secure 2024 election cycle also appreciate the committees' joint efforts to help protect our democracy and increase awareness of these important issues.

Today, I will 1) provide an overview of how AI may impact election administration and election officials, 2) share examples of AI-generated assets, 3) identify steps that election officials can take to protect against the threats posed to election administration, and 4) provide information we have collected from election officials in our annual local election official survey and other methods about their experiences with AI.

[1] The Brennan Center for Justice at New York University School of Law is a nonpartisan public policy and law institute that works to reform, revitalize, and defend our country's system of democracy and justice. I am a deputy director of the Brennan Center's Elections and Government Program. My testimony does not purport to convey the views, if any, of the New York University School of Law.

I. How AI may impact elections and election officials

Generative AI has added a new and complex dimension to the existing threats to election offices and election vendors. It excels at imitating authoritative sources, making it easier to deceive specific individuals or the general public by impersonating election officials or forging official election documents, and it can do so on a massive scale. As Harvard University professor Bruce Schneier has noted, artificial intelligence will increase the "speed, scale, scope, and sophistication" of threats to our democracy.[2] Put another way, many of the threats are not new, but they could become more dangerous in the rapidly evolving AI environment. For the 2024 U.S. election, the real challenge is that AI provides agitators new tools to increase the scale of such attacks at little cost and in more sophisticated form than we have previously seen. This means, in addition to their other efforts to administer a safe and secure 2024 election, election officials are learning to identify, prepare for, and respond to AI-related threats.

II. Examples of AI-generated assets

Mere awareness of the ways that AI might threaten elections is no substitute for actually seeing how it could do so. As part of our work on AI and elections, the Brennan Center has partnered with election officials across the country to conduct tabletop exercises (TTXs). These are crisis scenario planning exercises, which bring together various government officials and others to practice coordinated responses to simulated challenges or crises ("scenarios"). In these exercises, we included examples of how AI could be used to disrupt elections, showing officials real AI-generated content. Most of the scenarios we used could have happened without AI—but now, agitators can more easily launch attacks on elections and on a much larger scale.

There are five main types of generative AI outputs that election officials should prepare for: audio, images, text, video, and malware. In our report, *How Election Officials Can Identify, Prepare for, and Respond to AI Threats* ("AI Report"), we include many of the AI-generated digital assets used during these exercises. They are included in Attachment 1. Below is a brief description of a small selection of the examples provided in Attachment 1.

- Deepfake videos

Deepfake videos (videos manipulated by AI) are one of the more advanced types of AI output. While the technology is improving at a rapid pace, deepfake videos are harder to create than simple text-based outputs and easier to spot as fake than other AI-manipulated content. Using only cheap tools easily available online, California's Institute for the Future generated a deepfake of Arizona Secretary of State Adrian Fontes, explaining the threats that AI poses. Videos like this one could be used by bad actors to impersonate election officials and spread misinformation about when, where, or how to vote.

[2] Bruce Schneier, "Will AI Hack Our Democracy?," Schneier on Security, Summer 2023, https://www.schneier.com/essays/archives/2023/07/will-ai-hack-our-democracy.html.

- AI-generated images

AI can easily generate realistic images in response to simple text prompts. These images can be used to disrupt the election in multiple ways. For example, an AI-generated image with a map of inaccurate drop box locations could be spread by well-intentioned community members to large networks, via WhatsApp or other messaging services.

- Deepfake audio

Deepfake audio (audio manipulated by AI) technology currently produces relatively high-quality deepfakes compared to deepfake video technology. Using publicly available audio, bad actors could clone an election official's voice, and send instructions about administering elections to poll workers or other election staff. Separately, this technology could be used to create hundreds of AI-generated generic voices to call election offices with questions, flooding their phone lines and disrupting their work.

- Spoofing official websites, emails, or social media accounts

Simple AI tools like ChatGPT can be used to copy election office websites or their official social media accounts and provide false information about elections. For example, these sites or accounts could spread fake cast vote records that fan the flames of conspiracy theories about elections.

III. Steps election officials can take to prepare for and respond to AI Threats

Election officials can take – and many have taken – multiple steps to prepare for and respond to AI threats. Crucially, election officials cannot do this alone. The most effective responses to these threats require the assistance and cooperation of government officials, community groups, members of the public, and others.

Here are the steps election officials can take ahead of the 2024 election, which are further explained in our AI Report:

1) Understand what AI can do.
2) Take control of official online presence.
3) Prepare for rapid-response communications.
4) Adopt cybersecurity and physical security best practices.
5) Build and strengthen relationships with local media and other partners.
6) Create escalation plans.
7) Prepare legal support networks.

IV. Election officials' concerns and experiences with AI

The future is here. According to the Brennan Center's 2024 survey of local election officials from across the country, seven (7) percent of local election officials are currently using AI.[3] Reported usage includes drafting social media content or press releases, locating polling sites, and translating materials into different languages. Thirteen (13) percent of local election officials have been approached by a vendor or outside group with products advertised as using artificial intelligence.

In the current environment, it's not surprising that in response to a question about whether guidelines by federal, state, or local agencies for the use of AI would be helpful, many local election officials (33%) indicated it would be helpful, while forty-five percent responded, "I don't know."

V. Conclusion

For years, experts have been warning about the threats that AI poses to elections — even before recent advancements — including those from misinformation directed at the public, phishing attacks against election offices, and other attacks against election infrastructure. Many election offices have already implemented significant and successful steps to protect their infrastructure and staff from these threats. Early conversations and awareness about AI's capabilities and how to prepare for worst case scenarios will help election officials build on their preexisting security plans to prepare for the more sophisticated and widespread attacks that AI may bring. To most effectively respond to these threats, election officials will need the assistance and cooperation of other government officials, community organizations, members of the public, and others.

[3] Brennan Center for Justice, *Local Election Officials Survey—May 2024*, May 1, 2024, https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-may-2024.