CALIFORNIA LEGISLATURE

STATE CAPITOL
SACRAMENTO, CALIFORNIA
95814

Joint Informational Hearing

Senate Committee on Elections & Constitutional Amendments and
Assembly Committee on Elections
Senator Blakespear and Assemblymember Pellerin, Chairs

Tuesday, June 4, 2024
Upon Adjournment of the 9:00 a.m.
Senate Committee on Elections and Constitutional Amendments Hearing
1021 O Street, Room 2100
Sacramento, CA 95814

Artificial Intelligence and Elections: Protecting Democracy in the Digital Era

Introduction

Deceptive images designed by their creators to influence the public have been around since humans first learned to draw. However, in today's technologically advanced society, the ease with which people can create and spread mis- and disinformation creates a world where many people may have trouble determining what is fact and what is fiction. The development of increasingly advanced artificial intelligence (AI) tools has made once time-consuming activities much easier to complete, while also enabling the completion of tasks that are otherwise too complex for humans to tackle alone. AI tools could almost certainly help with voter education and outreach efforts, improve the delivery of election-related materials, and much more. However, there are also drawbacks to the widespread availability of this technology. Any person with an internet connection can create realistic content to falsely portray an idea, spread incorrect information, and encourage action based on unsubstantiated information. Policymakers around the country are wrestling with how best to regulate this advancing technology. This hearing is designed to encourage a discussion and inform lawmakers and the public about proposals to regulate the use of AI in elections and about the challenges faced by people – and elections officials in particular – when trying to identify and regulate deepfakes, AI-generated content, and mis- and disinformation.

Preparing at the Local Level

In the United States, elections are locally administered and in California, this is typically done at the county level. With 58 counties, this means there are 58 different ways of administering elections. While the Legislature establishes election laws and the Secretary of State provides direction as the state's chief election officer, each county has its own set of challenges when it comes to identifying issues and mitigating threats. Having a decentralized election system has benefits, including making it more difficult to improperly alter election outcomes. It also means, however, that each county must tailor its own election system to protect against threats to the fair and accurate conduct of elections, including those posed by the use of deepfakes and AI-generated content. In order to prepare for potential threats, election offices work to plan and prepare well in advance of every election.

One example of this type of advance planning can be found in Arizona. In December 2023, the Arizona Secretary of State, in collaboration with the Brennan Center for Justice, the Institute for the Future, and the Elections Group conducted a tabletop exercise on how AI could disrupt elections in 2024. This was a planning exercise where participants responded to simulated emergency situations such as:

- Attempts to harvest county office login credentials using AI-generated emails and text messages that appeared to be from the state's election security office;
- An audio deepfake from a state official directing offices to keep polling locations open because of a nonexistent court order; and
- AI-generated photos purporting to show an election official involved in criminal activity circulating on social media.

In every case, the AI tools used to simulate the exercise were available on the web for free or at low cost and did not require special technical skills to operate.

The exercise included participants from 14 of Arizona's 15 counties, including county election officials and representatives from county information technology offices, along with law enforcement, emergency management services, federal and state agencies such as the Cybersecurity and Infrastructure Security Agency and the National Guard, and other members of the elections community. Following the exercises, one major conclusion was the need for and importance of reinforcing fundamental security measures, such as implementing multifactor authentication, securing essential communication channels, conducting regular impersonation checks, and creating rapid-response communications plans.

Earlier this month, the Brennan Center for Justice and the Elections Group published a checklist to highlight the most achievable steps election officials can take now to mitigate AI threats before the 2024 general election. These include being familiar with AI content, having control of the office's online presence, adopting best practices for cyber and physical security, fostering relationships with technical service partners, creating escalation plans, and preparing legal support networks in case legal remedies are needed.

State Action – Current Tools and Laws

In 2018, the Legislature approved and Governor Brown signed AB 3075 (Berman), Chapter 241, Statutes of 2018 to establish the Office of Elections Cybersecurity (OEC) in the Secretary of State's office. The OEC has two primary missions. First, it is responsible for coordinating efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections in California. The OEC is also tasked with monitoring and counteracting false or misleading information regarding the electoral process that is published online or on other platforms that may suppress voter participation, cause confusion, or disrupt the ability to ensure a secure election. According to the OEC's website, the office serves California with the sole purpose of keeping every Californian's vote safe from online interference, especially the spread of mis- and disinformation.

In 2019, the Legislature approved and Governor Newsom signed AB 730 (Berman), Chapter 493, Statutes of 2019. AB 730 sought to address concerns that deepfake technology could be used to spread misinformation in political campaigns. (Legislative analyses of AB 730 described "deepfake technology" as software capable of producing a realistic looking video of someone saying or doing something they did not actually say or do.)

AB 730 prohibits anyone from distributing deceptive audio or visual media with actual malice and the intent to injure a candidate's reputation or to deceive a voter, unless the media includes a disclaimer that it has been manipulated. AB 730 does not apply exclusively to deepfakes, but rather applies to any intentional manipulation of audio or visual images where a reasonable person would be misled into believing it was authentic. Notably, AB 730 focused on materially deceptive representations of *candidates*, and not on deceptive media of other aspects of the electoral process.

AB 730 included a January 1, 2023 sunset date, but the Legislature approved AB 972 (Berman), Chapter 745, Statutes of 2022, extending the sunset date to January 1, 2027.

California Initiative for Technology and Democracy

In November 2023, the nonprofit organization California Common Cause established the California Initiative for Technology and Democracy (CITED) to search for state-level solutions to the threats that disinformation, AI, deepfakes, and other emerging technologies pose to democracy and elections.

Specifically for California, CITED is intended to supply policymakers, the news media, and public at large with impartial expertise necessary on these issues. CITED intends to provide analysis of policy proposals, make policy recommendations, host events on the intersection of democracy and technology, and be a public resource.

In January 2024, CITED published a white paper, *Democracy on Edge in the Digital Age: Protecting Democracy in California in the Era of AI Powered Disinformation and Unregulated*

Social Media. The white paper noted the rise of AI-generated content around the world and the need for legislative action. As a result, the white paper recommended that California's policymakers enact sensible safeguards to ensure transparency, accountability, and oversight of social media companies and AI in order to protect elections while minimizing impacts to technological innovation.

Tech Accord to Combat Deceptive Use of AI in 2024 Elections

In February 2024, 20 technology companies signed the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections." This set of commitments seeks to combat harmful AI-generated content meant to deceive voters. The signatories included Adobe, Amazon, Anthropic, Arm, ElevenLabs, Google, IBM, Inflection AI, LinkedIn, McAfee, Meta, Microsoft, Nota, OpenAI, Snap Inc., Stability AI, TikTok, Trend Micro, Truepic, and X.

The aforementioned companies signed the accord as a voluntary framework to advance seven goals:

1) Prevention: Researching, investing in, and/or deploying reasonable precautions to limit risks of deliberately deceptive AI election content being generated.
2) Provenance: Attaching signals to identify the origin of content where appropriate and technically feasible.
3) Detection: Attempting to detect deceptive AI election content or authenticated content, including using methods such as reading provenance signals across platforms.
4) Responsive Protection: Providing swift and proportionate responses to incidents involving the creation and dissemination of deceptive AI election content.
5) Evaluation: Undertaking collective efforts to evaluate and learn from the experiences and outcomes of dealing with deceptive AI election content.
6) Public Awareness: Engaging in shared efforts to educate the public about media literacy best practices, in particular regarding deceptive AI election content, and ways citizens can protect themselves from being manipulated or deceived by this content.
7) Resilience: Supporting efforts to develop and make available defensive tools and resources, such as AI literacy and other public programs, AI-based solutions (including open-source tools where appropriate), or contextual features, to help protect public debate, defend the integrity of the democratic process, and build whole-of-society resilience against the use of deceptive AI election content.

With these goals in mind, the signatories committed to taking the following steps through this year:

1) Develop and implement technology to mitigate risks related to deceptive AI content.
2) Assess and better understand the risks presented by deceptive AI election content.
3) Seek ways to detect the distribution of deceptive AI election content.
4) Seek to address deceptive AI election content.
5) Share best practices and explore pathways to share tools throughout the industry.
6) Provide transparency to the public.

7) Continue to engage with stakeholders to better understand the global risk landscape.
8) Support efforts to raise public awareness regarding deceptive AI election content.

Pending Legislation

According to the National Conference of State Legislatures, 16 states (Alabama, Arizona, California, Colorado, Florida, Idaho, Indiana, Michigan, Minnesota, Mississippi, New Mexico, Oregon, Texas, Utah, Washington, and Wisconsin) enacted legislation designed to address deceptive media, including but not limited to, AI.

As it relates to AI and elections in California, there are three bills being considered by the Legislature that seek to address deceptive and digitally altered elections-related content in an effort to protect the integrity of elections in California:

- AB 2355 (W. Carrillo) requires disclaimers to be put on paid political advertisements that are generated or substantially altered using AI. AB 2355 targets content generated by AI that falsely appears to be authentic to a reasonable person, or that is materially altered by AI in a way that causes a reasonable person to have a fundamentally different understanding of the altered media compared to an unaltered version. AB 2355 is awaiting assignment by the Senate Committee on Rules.

- AB 2655 (Berman) requires large online social media platforms to block the posting or sending of materially deceptive and digitally modified or created content related to elections, or to label that content, before and after an election. AB 2655 aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also elections officials and elected officials who are not candidates. AB 2655 also targets media that portrays elections materials and equipment in materially deceptive ways. AB 2655 is awaiting assignment by the Senate Committee on Rules.

- AB 2839 (Pellerin) of 2024 prohibits the distribution of campaign advertisements and other election communications containing materially deceptive and digitally altered or created images or audio or video files with the intent to influence an election or solicit funds for a candidate or campaign. AB 2839 aims to regulate materially deceptive and digitally altered media depicting not only candidates, but also depicting elections officials and elected officials who are not candidates, and election materials and equipment. AB 2839 is awaiting assignment by the Senate Committee on Rules.

Conclusion

Deceptive AI-generated and altered election content will become more prevalent as technology improves and evolves. Many stakeholders – government and elections officials, private technology firms, election integrity groups, and many others – are engaged in finding solutions to these challenges. The purpose of this hearing is to inform and assist the Legislature in making informed decisions on legislation related to AI-generated and altered content.