The Federal and State Legislative Landscape on the Use of Artificial Intelligence in Elections

Sept. 12, 2024

Sanam Hooshidary | Legislative Specialist
Adam Kuckuk | Policy Associate

As we enter election season, the federal government and states are concerned about the role artificial intelligence is playing in campaigning and what impact it could potentially have for November 2024 elections.

Congress and the states recognize there are benefits AI can bring to the election process, but are leery of its potential hazards. This paper explores the approaches Congress and the states are taking to address AI's influence on both federal and state elections.

FEDERAL ACTIONS

Both Congress and the administration have grappled with how to address the impact AI could have on federal elections. The rapid development and rollout of AI has spurred a flurry of federal activity centered around keeping the nation's elections processes safe and accurate. Policymakers recognize AI offers positive benefits and are open to using this powerful technology to protect elections by detecting and mitigating cyber threats, examining disinformation, and fact checking information provided by campaigns. They also understand that, in the campaign space, candidates can implement AI technologies to analyze and review large datasets that identify voter behavior patterns and help campaigns develop more targeted messages and slogans.

At the same time, legislators and regulators realize they cannot lose sight of the challenges the use of AI can bring to the election and campaigning process, including significant concerns related to facilitating voter suppression and spreading misinformation.

In the elections space, as in other AI use cases, legislative efforts attempt to balance the benefits of AI with its challenges, namely the capability to compromise campaigns and electoral reliability. Recently introduced federal legislation seeks to rein in nefarious uses of AI in elections, as well as establish clear rules, and ensure transparency essential to the democratic process.

LEGISLATION INTRODUCED IN THE 118TH CONGRESS ADDRESSING THE USE OF AI IN ELECTIONS

S. 2770 and **H.R. 8384**, the Protected Elections from Deceptive AI Act, seeks to prohibit the distribution of materially deceptive AI-generated media, particularly political advertisements, related to federal candidates. It focuses on preventing AI-generated content that misleads voters or manipulates election outcomes.

S. 3875, the AI Transparency in Elections Act of 2024, mandates that political advertisements containing AI-generated content include a disclaimer indicating the use of AI. It establishes guidelines for monitoring and examining AI systems used in election-related activities to warrant transparency and prevent manipulation.

S.3897 and **H.R. 8353**, the Preparing Election Administrators for AI Act, requires the U.S. Election Assistance Commission to develop guidelines to help election officials manage AI's risks and applications in elections. It includes provisions for training programs, resource allocation and the development of best practices to safeguard the electoral process against AI-driven threats.

H.R. 4611, the Candidate Voice Fraud Prohibition Act, pertains to campaigns and prohibits the distribution of paid political communications that contain materially deceptive audio generated by AI, especially when used to mislead voters or manipulate public opinion, making it a crime to do so. The bill contains criminal penalties of up to two years in prison, a fine or both.

H.R. 6936, the Federal Artificial Intelligence Risk Management Act of 2024, focuses on managing AI risks, including its use in electoral processes. The bill mandates the creation of standardized risk management protocols, regular audits and transparency measures to ensure the responsible utilization of AI technologies. Additionally, it requires federal agencies to report on their use of AI and compliance with risk management practices to Congress.

H.R. 8858, the Securing Elections From AI Deception Act, prohibits the use of AI to deprive or defraud individuals of the right to vote in elections for public office. This bill prohibits the use of AI-generated content and requires political campaigns and third-party groups to disclose if AI was used to create or edit any sort of content shared with the public. In addition, it requires the Federal Election Commission and other related federal agencies to regulate bodies to monitor the interference of AI used in elections.

H.R. 8668, the AI Transparency in Elections Act of 2024, amends the Federal Election Campaign Act of 1971 to provide transparency for the use of content substantially generated by AI in political advertisements. This bill would require advertisements to include a statement noting that AI was used to generate content seen in the advertisement. For transparency reasons, campaigns are also required to report to the Federal Election Commission any AI use in their content and the type of AI tools used. This act aims to protect voters from being misled by AI-generated deepfakes or other deceptive content.

RECOMMENDATIONS FROM THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) is responsible for helping the United States protect and defend against cyber risks and risks to the country's critical infrastructure. The work of CISA is informative for helping policymakers and election officials understand how AI could impact the security and integrity of our elections.

In the report Risk in Focus: Generative AI and the 2024 Election Cycle, the agency has identified four known tactics bad actors can use to disrupt and cause chaos in U.S. elections with examples of how these tactics could be used. CISA describes them as text-to-video or deepfake, text-to-image or AI-altered image, text-to speech or voice cloning, and text-to-text or large language models. These AI-generated content can weaken the democratic process and mislead voters through disinformation, phishing campaigns and promoting foreign influence. CISA maintains that deepfake videos could create fabricated representations of candidates, spreading misinformation and possibly harming candidates' reputations. Chatbots could misrepresent the time and place of an election. Voice cloning could impersonate election staff to gain access to voter databases. AI can also have micro-targeting effects on voters through misinformation, which can intensify biases and influence voter opinions.

While not official guidance, CISA recommends strategies that policymakers, candidates, election officials, and the public can take to mitigate the risks of election interference such as installing strong cybersecurity protocols, securing personal

social media accounts by making them private, incorporating strong and verifiable technical controls that weed out inauthentic access requests, and building a strong network of trusted media and community. As the U.S. navigates toward a more AI-driven society, understanding and implementing these recommendations could be crucial to maintaining the integrity of the electoral process.

STATE ACTIONS

AI is only the latest wrinkle in a long line of technological changes to impact state campaigns and elections. Candidates, campaign staff and election administrators have always adapted to new technologies, from political television ads in the mid-20th century to the recent rise of cryptocurrency contributions.

With the 2024 elections quickly approaching, state policymakers have been contemplating how to regulate this technology in a presidential election year. Only a few bills have been introduced addressing AI in election administration processes, most notably Arizona's 2024 SB 1360, which would have prohibited machines used in elections from using AI. Political messaging bills have seen more activity in the years leading up to the 2024 election.

Since 2019, at least 19 states have enacted laws regulating AI's use in political messaging. There have been three main considerations in AI political messaging legislation: How should these bills define AI, what regulatory provisions should be included and what enforcement provisions should look like.

HOW HAVE STATES BEEN DEFINING AI IN THE CONTEXT OF CAMPAIGNING AND POLITICAL MESSAGING?

AI is challenging to define due to its complexity and evolving nature. AI is composed of various computer algorithms that vary from program to program. As a result, there is no universally accepted definition of AI. States may use different terms such as synthetic media, deceptive media, deepfake or a variety of others that encompass the deceptive use of media to influence an election.

Some states have attempted to define "artificial intelligence" directly. Florida defines generative AI as "a machine-based system that can, for a given set of human-defined objectives, emulate the structure and characteristics of input data in order to generate derived synthetic content." New Mexico defines AI as "a machine-based or computer-based system that through hardware or software uses input data to emulate the structure and characteristics of input data in order to generate synthetic content, including images, video or audio."

Other states use definitions that may encompass AI without using that exact phrase. Minnesota defines a "deepfake" as an image, audio or video that's production was "substantially dependent upon technical means" rather than an individual's physical or verbal ability to impersonate someone.

In the political messaging context, states have used various terms to reference AI-generated content such as "synthetic media," "deepfake," "materially deceptive media" and "doctored media." These terms may have different definitions state to state. For example, Wisconsin and Washington both use the term "synthetic media." Wisconsin defines synthetic media as including audio and video, while Washington includes audio, video and images. Similarly, California and Michigan both use the term "materially deceptive media," but only Michigan requires the media to have been generated by AI.

States' definitions may cover more than just AI. California uses the term "materially deceptive media," defining it as the confluence of two conditions: 1) a reasonable person would believe the media is authentic; and 2) a reasonable person would have a fundamentally different understanding of the media if it were unaltered. This definition makes no mention of technology, and thus may apply to any misleading or false content, whether generated by AI or otherwise.

Idaho and Washington both define synthetic media as using "generative adversarial network techniques or other digital technology." Generative adversarial networks (GANs) are one of several underlying models that AI uses to generate content, with diffusion models being another example. Because GANs are only one of many models, these definitions may not capture all AI-generated content.

Most states' laws regulate AI by focusing on the medium by which AI is distributed: audio, images and/or video. Many states include all three media, but some only include one or two. Texas passed legislation in 2019 defining deepfakes as videos, notably leaving out other media. This has left the law's applicability to audio and images unclear.

WHAT PROVISIONS ARE STATES INCLUDING TO REGULATE AI'S USE IN POLITICAL MESSAGING?

States have taken several legislative approaches to regulate AI in political messaging. However, no state has a complete ban on deceptive AI-generated political messaging, likely due to First Amendment concerns. New state laws establish durational prohibitions, disclosures and some states have used current law to address deceptive practices.

Though full prohibitions do not currently exist, two states only have durational prohibitions. These laws make it a crime to publish deepfakes intended to influence an election within a specified window of time. Minnesota prohibits the publication of deepfakes 90 days prior to an election and Texas prohibits publishing a deepfake video 30 days prior to an election.

By far the most common approach to regulation has been requiring disclosures. Most state campaign finance laws require disclosures on ads identifying the committee or person who funded it. Similarly, AI disclosures require content to include text stating it was generated by AI.

Disclosures and durational prohibitions can work together. Disclosure requirements often include durational prohibitions but allow the content to still be published so long as the disclosure is included. For example, Arizona prohibits deceptive AI-generated content 90 days prior to an election, unless the message includes a "clear and conspicuous disclosure" that the content was generated by AI. Washington on the other hand does not include a duration requirement and disclosures must be included on political deepfakes published year-round.

Another approach is to include digitally embedded disclosures. These types of disclosures require information to be contained in a digital file's metadata: descriptive information about a file's creator, when the file was created, when the file was edited, etc. Colorado and Utah both require AI-generated content to contain metadata about the program that was used to create it, who created it, when it was created and a disclosure stating it was created by AI. This requirement allows news and social media sites that have these images uploaded to their platforms—or any person who wants to—the ability to independently verify the media's authenticity.

AI laws may not be needed in some states as their current laws may already cover unwanted conduct. In early 2024, New Hampshire residents received an AI-generated phone call that sounded like President Joe Biden telling voters not to vote. At the time, New Hampshire did not have an AI political messaging law, so the New Hampshire Attorney General's Office instead charged the political consultant behind the calls with 13 counts of voter suppression and 13 counts of impersonation of a candidate. In August 2024, New Hampshire enacted HB 1596 to require the disclosure of deceptive AI usage in political advertising.

To avoid First Amendment violations, some states built in exceptions to the applicability of their laws. One example is New York, which exempts satire or parody. Another exception is for media providers. In Wisconsin, liability for damages is waived for broadcasters or online platforms so long as they didn't create the content.

HOW DO STATES ENFORCE THESE POLICIES AND ARE THERE PENALTIES FOR VIOLATIONS?

Most of the legislation on AI in political messaging includes some form of civil or criminal penalty for violating their AI political messaging laws. However, none of these laws have been widely tested in courts.

Many states have chosen to leave enforcement to civil courts. Candidates in most states can seek injunctive relief to prohibit the further publication of an AI-generated image of themselves. Some states, like Mississippi, have extended a cause of action for the "wrongful dissemination of digitizations" to other individuals who may have been falsely depicted, like lay people or other public officials.

Several states allow candidates to seek repayment of court costs and damages if they are either the subject of a frivolous lawsuit or prevail in court on the merits. Due to the increasing sophistication of AI content, people may bring lawsuits against real content claiming it is fake. Alabama has attempted to remedy this by allowing a defendant to obtain court costs and attorney's fees for frivolous lawsuits as well.

States may choose to impose civil penalties. New Mexico and Utah fine offenders $1,000 for each violation for disseminating materially deceptive media and synthetic media, respectively. Colorado's civil penalty may include imposing a penalty of 10% of the dollar amount used to promote a deepfake.

About a third of the states that have enacted laws also have criminal penalties specific to their AI political messaging laws. Although more uncommon than other penalties, some states have punishments of prison time. For example, Texas's law allows a maximum sentence of one year in prison for a violation. Some prison sentences are tied to specific conditions such as in Minnesota where second violations have longer maximum sentences. In Mississippi, violations intended to cause violence can be given a maximum of five years, whereas all other violations carry a maximum of one year.

Some states also have criminal fines that can be imposed with, or instead of, prison time. Michigan's fine of $500 for the first violation is among the nation's lowest, while Minnesota's fine of $10,000 for second violations is one of the largest.

CONCLUSION

AI is rapidly influencing elections in this country and worldwide. While technology offers considerable potential, it also poses risks, particularly in the form of disinformation, deepfakes, and voter suppression. Leaders in federal and state government are responding by outlining strategies and enacting new laws to mitigate harm from deceptive AI election content. As legislative leaders explore policy options, some considerations to keep in mind are:

- First Amendment implications.
- Types of media that are being regulated (audio, video or images).
- Types of penalties imposed for violations (civil or criminal).
- Federal agency or congressional preemptions.