# THE ROLE OF STATE ATTORNEYS GENERAL IN PROTECTING ELECTIONS FROM INTERFERENCE THROUGH ARTIFICIAL INTELLIGENCE AND ROBOCALLS

Rapid advancement and public availability of machine learning and artificial intelligence (AI) have spurred both federal and state officials to develop policies governing its use, including in the realm of elections. In a highly contested presidential election year such as 2024, exploitation of technology to produce "deep fake" media[i] poses grave risks of deceiving voters and impacting the outcome of elections through deception. While authorities are moving quickly to fill the policy gap, state Attorneys General are using legal tools both old and new to protect the public and election processes against nefarious actors seeking to deceive voters.

## Federal Action

The Biden Administration issued an expansive Executive Order in October 2023 on safe and appropriate use of AI.[ii] Deploying a whole-of-government approach, the order directs federal agencies to establish guidelines and best practices for developing and deploying AI systems. With respect to political processes, agencies must develop methods to protect critical infrastructure including election infrastructure, as well as requirements that will identify, label, and protect the public against misuse of synthetic, AI-generated content.[iii]

To that end, the Federal Communications Commission (FCC) issued a Notice of Inquiry in November 2023, seeking public input into consumer protections against robocalls and robotexts that use AI technology. These forms of communications are prohibited without express consent from a consumer under the Telephone Consumer Protection Act (TCPA), which is largely enforced by state Attorneys General.[iv] In response, a bipartisan group of 26 state Attorneys General submitted a letter asking the FCC to adopt a definition of AI that would define any type of AI technology that generates a human voice as an "artificial voice" for purposes of the TCPA, thereby requiring prior express written consent.

On February 8, the FCC did just that when it released a Declaratory Ruling affirming that TCPA's prohibitions against an "artificial or prerecorded voice" apply to AI-generated content that resembles a human voice. Now, in addition to prohibiting unsolicited robocalls, the TCPA also bans using AI to generate a voice played in such calls, expanding avenues for enforcement by state Attorneys General.

## State Enforcement

The close partnership between federal and state actors in enforcing federal consumer protections against deep fakes was exemplified in early 2024 in New Hampshire. In the days leading up to the January 23, 2024, Presidential Preference Primary, a robocall using an AI-generated voice cloning President Biden was placed to more than 20,000 voters urging Democrats not to vote in the primary. The New Hampshire Attorney General's office announced that it had identified the source of the robocall, and both state and federal officials issued cease and desist orders and began criminal investigations.

The 51-member Anti-Robocall Multistate Litigation Task Force, consisting of every state Attorney General along with the District of Columbia, issued a warning letter to the corporation responsible for the New Hampshire deep fake robocall. The letter identified other federal consumer protection laws that also apply,[v] including the Truth in Caller ID Act in the case of "spoofing" a false outgoing number, [vi] and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[vii] Warning letters like these serve notice not only to the parties responsible for the call, but to any other party considering these tactics that state Attorneys General are prepared aggressively to pursue charges against wrongdoers to protect the integrity of election processes.

**State AI Policies**

While federal law provides important tools to protect against use of AI to mislead voters, several states have passed their own laws to protect election processes from deep fakes. Some of these include:

- **Michigan** passed a series of bills [viii] that prohibit the use of content generated by AI in political advertising without disclosing the source of the content. Criminal penalties apply for the distribution of deep fakes within 90 days of an election with the intent to influence the outcome of an election, and without disclosing the fact that the image, video, or audio was manipulated and depicts "speech or conduct that did not occur.[ix]

- **Washington State** likewise prohibits distributing electioneering communication containing "synthetic media" without disclosure.[x] In addition to empowering the state Attorney General to enforce these restrictions, Washington's law also allows any candidate whose appearance, action, or speech is altered through synthetic media to seek an injunction prohibiting publication, as well as damages.

- **California** state law prohibits, within 60 days of an election, distribution without disclosure of deceptive media with intent to injure a candidate's reputation or deceive a voter.[xi] Any candidate whose likeness is portrayed in violation of these prohibitions may seek injunctive relief as well as damages.

- **Minnesota** passed a law in 2023 criminalizing the dissemination within 90 days of an election of a "deep fake" designed to harm a candidate or influence an election.[xii] In addition to criminal penalties, the law grants standing to the depicted individual and any candidate who is injured to seek injunctive relief.[xiii]

**Other Avenues for Relief**

Although AI-powered deep fakes pose a unique threat to the integrity of elections, the broader category of disinformation and fraud has long been a scourge in elections, and most states have robust legal protections that can be deployed to protect elections and voters even in the absence of AI-specific legislation.

- **Wisconsin**, for instance, has long prohibited false representations pertaining to a candidate or referendum intended to affect voting.[xiv]
- **New Jersey** election law likewise prohibits inducing a voter's behavior by means of any fraudulent device or contrivance.[xv]

Attorneys General may directly enforce these and other relevant laws, such as broad consumer protection laws against deceptive practices. In other instances, state Attorneys General may represent their states' chief election offices in enforcement actions.

## Conclusion

Cutting edge technologies are often double-edged swords, offering as many threats as opportunities. While policymakers recognize the risks that AI-produced synthetic media poses to our democracy and are scrambling to mount a response, state Attorneys General have tools at their disposal to hold accountable malicious actors who attempt to interfere in elections through disinformation.

---

[i] *See, e.g.,* Minn. Stat. 609.771 (c):

> (c) "Deep fake" means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof:
>
> (1) that is so realistic that a reasonable person would believe it depicts speech or conduct of an individual who did not in fact engage in such speech or conduct; and
>
> (2) the production of which was substantially dependent upon technical means, rather than the ability of another individual to physically or verbally impersonate such individual.

[ii] Artificial Intelligence (AI) is defined under 15 U.S.C. § 9401(3) as follows:

> a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

[iii] Executive Order No. 14110 §§ 4.1(b), 4.5 (2023) (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/)

[iv] *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991), codified at 47 U.S.C. § 227.

[v] *See* Feb. 6, 2024 Notice Letter from Anti-Robocall Multistate Litigation Task Force, https://illinoisattorneygeneral.gov/News-Room/Current-News/State%20AG%20Task%20Force%20NOTICE%20Letter%20to%20LIFE%20CORP%20%28Feb.%202024%29.pdf?language_id=1.

[vi] 47 U.S.C. § 227(e).

[vii] 15 U.S.C. §§ 6101-6108.

[viii] Act No. 263, Public Acts of 2023, 102nd Legislature, State of Michigan (2023); Act. No. 264, Public Acts of 2023, 102nd Legislature, State of Michigan (2023); Act No. 265, Public Acts of 2023, 102nd Legislature, State of Michigan (2023); Act No. 266, Public Acts of 2023, 102nd Legislature, State of Michigan (2023).

[ix] Mich. Comp. Laws PA 1954, No. 116 § 168.932f (2024).

[x] Revised Code of Washington, Title 42.17a (2023).

[xi] *See* Cal. Leg. Stat. Elec. Div. 20 § 20010.

[xii] *See* Minn. Stat. § 609.771 (2023).

[xiii] *Id.*

[xiv] *See* Wis. Stat. § 12.05.

[xv] NJSA 19:34-29.