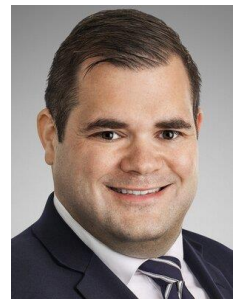


What State AI Election Laws Mean For The 2026 Midterms

By **Matthew Shapanka** (September 16, 2026, 4:33 PM EDT)

Artificial intelligence promises to reshape both politics and economics for generations. As AI tools rapidly improve and spread, the law has barely started to address their effects, including in elections.

With less than two months remaining before the 2026 midterm elections, state election law — like other AI regulations — remains a complex and underdeveloped patchwork across the country. Beyond so-called deepfakes — synthetically generated materials that appear so realistic as to deceive a reasonable voter — few election rules expressly address AI.



Matthew Shapanka

Laws written long before modern generative AI now govern most AI-assisted political activity, from synthetic ads to candidate avatars that converse with voters to paid influencers to voter data modeling.

While regulators scramble to address new harms, campaigns, their vendors and AI developers must address the risk that outdated rules written for other problems will apply to the modern AI-powered campaign.

The Paradigm: Deepfake Laws

Twenty-nine states have election deepfake laws in effect.[1] Federal courts have enjoined two states' deepfake laws: California's A.B. 2839 and A.B. 2655, and Hawaii's Act 191.[2] Most states require disclaimers for covered synthetic content, often during a defined election period. Many also authorize candidates or regulators to seek judicial relief.

For example, Minnesota Statutes Section 609.771 and Texas Election Code Section 255.004 prohibit specified AI-generated media during defined periods — after the start of absentee voting and within 30 days of an election, respectively.[3]

On the other hand, Article 2 of Maryland's Election Law, which was enacted in June, prohibits knowingly or recklessly creating, using or disseminating covered media that produces materially false election information and causes or is intended to cause certain election-related harm.[4]

Enforcement has started. In May, Michigan state Senate candidate Jason Tunney sought more than \$157,000 over allegedly unlawful deepfake videos.[5] In July, Arizona congressional candidate Joseph

Chaplik sued a super political action committee, alleging that attack ads defamed him and violated state disclosure rules for AI-generated political images.[6]

The first constitutional challenges to state deepfake laws suggest that targeted disclosure rules may fare better than broad restrictions on political content, although the case law remains limited. In 2025, the U.S. District Court for the Eastern District of California permanently enjoined California's A.B. 2839 on First Amendment grounds in *Kohls v. Bonta*. [7] A related judgment held that Section 230 of the Communications Decency Act preempted A.B. 2655's requirements that large online platforms block "materially deceptive content related to elections" and label certain other synthetic content during a specified election period.[8]

In January, the U.S. District Court for the District of Hawaii struck down Hawaii's Act 191 in *Babylon Bee v. Lopez*. [9] The California case *Babylon Bee v. Bonta*, which was filed in 2025, is currently on appeal before the U.S. Court of Appeals for the Ninth Circuit.[10]

Not All Synthetic Content Is Deceptive

Many state deepfake laws focus on realistic content likely to deceive voters. Others require labels for broader categories of AI-generated political advertising. Many were enacted after a January 2024 New Hampshire robocall, in which a cloned voice purporting to be then-President Joe Biden urged Democrats not to vote.[11]

Today, much more AI-generated campaign content is conspicuously artificial. In May, a viral video created by AI filmmaker Charlie Curran depicted Los Angeles in flames with California Gov. Gavin Newsom as a digitally rendered aristocrat, the incumbent Mayor Karen Bass as a Joker-inspired villain, and mayoral candidate Spencer Pratt as a Batman-like hero arriving to save the city.

Pratt, whose campaign said it had not commissioned the video, reposted it.[12] Unlike the Biden robocall, the Pratt video embraced its artificial creation and presented itself as cinematic parody rather than authentic footage.

However, Jason Law, who is a candidate for St. Charles County executive in Missouri, used the same conspicuously synthetic format for a different purpose, releasing a fully AI-generated ad that depicted his opponents making false statements.[13] Missouri does not have an election deepfakes law. Similar ads may also escape regulation elsewhere when they contain fabricated statements but are too stylized to satisfy a statutory deception standard or fall within a satire or parody exception.

Beyond Deepfakes: New Tactics Lack Clear Legal Boundaries

On Aug. 7, California state Sen. Scott Wiener announced that his congressional campaign would remove *ConnieChan.ai*, a parody chatbot that used the name and political persona of his opponent, San Francisco Supervisor Connie Chan.[14]

The site disclosed that the campaign had paid for it and described it as parody. But prompts concerning Chan's accent and citizenship produced responses from former House Speaker Nancy Pelosi — whose seat in Congress Wiener and Chan are vying for — and other elected officials condemning the site as racist and sexist. After the criticism, Wiener's campaign pulled down the site and announced that the billboards promoting it would come down.[15]

The Wiener campaign bot shows the limits of both deepfake laws and other regimes directed at AI-generated election content. California's S.B. 1001 — the B.O.T. Act — which took effect in 2019, prohibits any person from using a bot to, among other things, "influence a vote in an election." [16] While the California B.O.T. Act appears to apply more cleanly here, the law requires an explicit intent to deceive and treats a clear and conspicuous bot disclosure as a safe harbor.

Voter Contact: The Limits of Telecom Law

Campaigns are also deploying AI to extend their own voter reach, not just to attack opponents.

Candidates can create chatbots trained to speak and write like them, allowing campaigns to engage voters in personalized chats and text messages. [17] While the use of cloned voices on outbound calls may run afoul of federal telecommunications law, AI-generated text messages face a less settled regime.

The Federal Communications Commission has held that AI-generated voices are artificial under the Telephone Consumer Protection Act, or TCPA. [18] Covered calls using artificial voices generally require the recipient's prior express consent unless an exception applies. That is why the FCC imposed a \$6 million forfeiture on Steve Kramer, the political operative behind the Biden robocall, and separately reached a \$1 million settlement in August 2024 with Lingo Telecom, the carrier that transmitted the calls. [19]

The legal treatment of AI-generated text is less clear. The TCPA already regulates certain automated texts, but the FCC's artificial voice ruling does not appear to make a text message unlawful merely because AI generated its content. Campaigns must instead analyze the dialing technology, consent, sender-identification rules and applicable state law.

Paid Persuasion: Influencers and Synthetic Performers

As campaigns and political committees increasingly turn to online influencers — individual content creators who maintain a large social media audience — to distribute their political messages, disclosure rules have not kept pace.

In most cases, influencers paid by political organizations — including organizations that are not required to disclose their donors — to speak or post about the election are not required to report or disclose the source of the paid content. Some label their political posts as advertising, but without naming their funder.

Unlike in the commercial context, where Federal Trade Commission rules require disclosure, federal rules in the election law context do not require sponsorship disclaimers on every paid influencer post. [20] In December 2023, the Federal Election Commission declined to extend its internet disclaimer rules expressly to paid influencer content, over the dissent of two commissioners. [21]

States like California and Texas, on the other hand, have adopted rules — like California's S.B. 678 and the Texas Ethics Commission's Rule 26.1 — that require influencers to disclose payments for political content. [22]

The recent emergence of AI-generated influencers complicates this landscape. State influencer laws were written with human creators in mind and do not clearly explain how their disclosure rules apply when a campaign creates the synthetic persona itself. New York's S.B. S8420A, a new synthetic

performer disclosure law that took effect in June, applies to advertisements produced for a commercial purpose, and therefore does not supply a general disclosure rule for campaign advertising.[23]

Nor do state deepfake statutes necessarily close that gap: Synthetic personas are not automatically deceptive but could be used to create materially deceptive content.

Voter Data: The Limits of Privacy Law

AI has also unlocked new ways for campaigns to analyze the data that their political committees and parties accumulate from voter files, phone banks, canvassing, contribution histories and other sources. Comprehensive privacy laws often leave political data practices outside their scope, but campaigns do not operate in a legal vacuum. State voter file laws may restrict access to, disclosure of or permitted uses of registration data, while comprehensive privacy statutes vary in their treatment of nonprofit and political organizations.

The state privacy laws that regulate equivalent commercial conduct mostly do not apply: The California Consumer Privacy Act reaches only entities "organized or operated for the profit or financial benefit of its shareholders or other owners" and related entities or joint ventures made up of for-profit businesses, while privacy laws in Texas and Virginia include language exempting nonprofit organizations, which are defined to include political organizations.

Other states, including Colorado and New Jersey, offer no categorical exceptions for nonprofits or political organizations, leaving a patchwork of state laws in place governing the use of voter data.

Chatbots, Call Recordings and Wiretap Laws

In addition to data privacy laws, other privacy-like regimes may regulate the technologies campaigns use, often without an exemption for nonprofits or political organizations.

Campaign or issue websites that offer AI-chatbots or automated phone lines to answer voter questions may implicate state wiretapping laws, at least where the automated service is provided by a third-party vendor. This is an area of active privacy class action litigation around the country, with plaintiffs arguing that transmission of a chatbot message to a third-party vendor violates state laws that require all parties to an electronic communication to consent to a recording.

Courts, like the U.S. District Court for the Northern District of California in *Hubbard v. Google* **in January 2025**, have found that it is not enough to simply disclose the third-party vendor arrangement in a privacy policy linked in the footer of a website.[24]

Automated voice bots raise similar concerns. About a dozen states require all-party consent for the recording or interception of telephone calls, while the remaining states and federal law require only single-party consent.

Campaigns and political committees that deploy AI phone banks and other services that may record or transcribe caller interactions will need to ensure that they obtain the required consents in each jurisdiction where they operate.

Practical Tips for the 2026 Midterms

In the absence of federal rules governing AI in elections and no consensus emerging across state laws, many election use cases fall into uncertain legal territory. No consistent regime is likely to emerge before November, requiring AI developers, social media platforms and political committees to judge the risk of each campaign-related AI use.

Candidates and vendors deploying AI this cycle — and the platforms and developers whose products they use — can take some steps now to prepare for likely post-election investigations and litigation, as well as the legislation that will follow to fill the gaps.

- Many platforms already require disclosure of synthetic content in political ads released or generated on their platforms and police violations under their own terms of service. Companies that have not included election-related terms in their user agreements should consider adopting them quickly, before the election, to ensure compliance with relevant state AI laws and to prepare to defend against aggressive enforcement of pre-AI era laws.
- AI-generated content — including candidate impersonations, synthetic personas or other AI-generated material — could still expose campaigns to liability for defamation or violate the terms of service of particular platforms or AI tools, even if that AI use is disclosed. Users should carefully evaluate the risks of using AI to speak or write on behalf of a candidate or campaign and establish procedures for addressing false outputs.
- Campaigns and vendors should analyze TCPA and equivalent state law compliance requirements before deploying any AI-generated voice or text-messaging capabilities.
- Campaigns deploying AI website or phone chatbots to interact with voters should ensure that they secure consent from participants — both for the recording and the use of a third-party vendor — at the start of the chat or call, rather than rely on passive disclosures, like a link to a privacy policy.
- Political organizations should audit their AI vendor contracts to ensure that they include representations and warranties covering state wiretapping statutes for any vendor that records, receives or stores call audio or chat transcripts.
- Developers and platforms that impose election-related restrictions on users should document and apply those restrictions consistently.

State legislatures and campaign finance regulators will likely revisit many of these issues, but not before the 2026 midterms. In the meantime, the lawsuits and enforcement actions under current law will determine how policymakers approach new rules.

Stakeholders that prepare now will have a stronger record in future enforcement proceedings and policy debates.

Matthew S. Shapanka is of counsel at Covington & Burling LLP. He previously served as chief counsel for the U.S. Senate Committee on Rules and Administration.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their

employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns>.

[2] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2839; https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655; https://www.capitol.hawaii.gov/sessions/session2024/bills/GM1292_.PDF.

[3] <https://legiscan.com/MN/text/HF1370/id/2811480/Minnesota-2023-HF1370-Engrossed.pdf>; <https://legiscan.com/TX/text/SB751/id/2027638/Texas-2019-SB751-Enrolled.html>.

[4] https://mgaleg.maryland.gov/2026RS/Chapters_noln/CH_444_sb0141e.pdf.

[5] https://www.abc12.com/news/politics/republican-seeks-judgment-for-fake-ads-in-35th-district-senate-race/article_88e0b8dd-672d-4494-9d8a-a37d1fb83a10.html.

[6] <https://www.phoenixnewtimes.com/news/arizona-gop-congressional-hopeful-chaplik-sues-pac-attack-ads-40682453/>.

[7] <https://storage.courtlistener.com/recap/gov.uscourts.caed.453046/gov.uscourts.caed.453046.101.0.pdf>.

[8] <https://storage.courtlistener.com/recap/gov.uscourts.caed.453046/gov.uscourts.caed.453046.100.0.pdf>.

[9] <https://storage.courtlistener.com/recap/gov.uscourts.hid.174048/gov.uscourts.hid.174048.47.0.pdf>.

[10] <https://storage.courtlistener.com/recap/gov.uscourts.ca9.513de877-dff4-4a93-a3cd-c04e7834f4c4/gov.uscourts.ca9.513de877-dff4-4a93-a3cd-c04e7834f4c4.19.1.pdf>.

[11] <https://www.doj.nh.gov/news-and-media/steven-kramer-charged-voter-suppression-over-ai-generated-president-biden-robocalls>.

[12] <https://www.hollywoodreporter.com/news/politics-news/spencer-pratt-batman-ai-campaign-video-1236587741/>.

[13] <https://www.firstalert4.com/2026/07/20/ai-generated-political-ad-st-charles-county-raises-deepfake-questions-ahead-primary-election/>.

[14] <https://sfstandard.com/2026/08/06/wiener-built-ai-chatbot-mock-chan-s-politics-pelosi-says-s-sexist-racist/>.

[15] <https://www.kron4.com/news/bay-area/scott-wiener-says-conniechan-ai-chatbot-campaign-billboards-to-be-removed/>.

[16] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

[17] <https://www.whro.org/2026-07-12/political-text-messages-could-get-more-effective-and->

annoying-blame-ai.

[18] <https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf>; <https://www.fcc.gov/rules-political-campaign-calls-and-texts>.

[19] <https://docs.fcc.gov/public/attachments/DOC-405811A1.pdf>; <https://docs.fcc.gov/public/attachments/DOC-404951A1.pdf>.

[20] https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.

[21] <https://www.fec.gov/resources/cms-content/documents/Reg-2013-01-TechMod-Final-Statement-ELW-and-SMB.pdf>.

[22] <https://www.ethics.state.tx.us/data/search/rules/commission/Rules.pdf>.

[23] <https://www.nysenate.gov/legislation/bills/2025/S8420/amendment/A>.

[24] <https://storage.courtlistener.com/recap/gov.uscourts.cand.350532/gov.uscourts.cand.350532.318.0.pdf>.