

COMPLIANCE WEEK

FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

Election rules aimed to curb AI misuse may serve as regulatory warning for all advertisers



By [Adrienne Appel](#) | Mon, Nov 4, 2024 9:28 AM

With the presidential election this week, one fear has remained on the minds of voters regardless of their political stripe—that artificial intelligence (AI) will be misused to change the outcome of the race.

A majority of Americans worry about AI influencing the presidential election, according to a recent Pew Research Center [study](#).

And for good reason.

AI is relatively inexpensive and easy to use, and has spread like wildfire among legitimate businesses and bad actors. Once AI content is created, social media and the internet make it quick and easy to disseminate, said Samantha Rothaus, partner in Davis+Gilbert's advertising and marketing practice.

In one high-profile case of misuse, in June 2023, Florida Gov. Ron DeSantis (R) released fake, AI-created images of former President Donald Trump kissing Dr. Anthony Fauci, Trump's former chief medical advisor, according to the [New York Times](#).

In January of this year, thousands of New Hampshire primary election voters received phone calls from an AI-generated **robocall impersonating President Biden**. The fake voice told them not to vote. The FCC later proposed a \$2 million fine against Lingo Telecom for transmitting the calls, and a \$6 million fine against Steve Kramer, the political consultant who hired Lingo.

This summer, Trump's campaign grossly misused an image of Taylor Swift to make it appear she endorsed him, when she had not, **CNN** reported. And Elon Musk re-tweeted a fake video of Vice President Kamala Harris, in which AI cloned her voice and made it look like she was making statements she never uttered, according to the **Associated Press**.

Meanwhile, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), issues near-constant **warnings** about attempts by threat actors outside the U.S., some acting on behalf of other nations, to use sophisticated AI images to influence or dismantle U.S. elections.

More than 25 states quickly enacted laws to regulate the use of AI in elections, according to **Public Citizen**. Federal regulators have struggled to catch up to the lightening speed of AI.

"There is a greater risk because the tools are easily accessible and it's easy to get false messages out there," said Liz Corradino, partner at Moses Singer.

AI "could shape the political landscape of elections if we don't put some guardrails around how generative AI is used and what disclosures need

to be made,” Singer said.

On February 2 the FCC issued a **declaratory ruling**, effective immediately, that robocalls using AI-generated content fell under the jurisdiction of the Telephone Consumer Protection Act. The ruling made clear that any businesses using AI voices need to obtain prior consent of potential recipients before they can be called with content that includes AI-created voices.

On July 25, the FCC **proposed a rule** to require disclosure if AI is used to create political ads aired on radio and TV.

The draft rule is “a major step to guard against AI being used by bad actors to spread chaos and confusion in our elections,” FCC Chairwoman Jessica Rosenworcel said.

“There’s too much potential for AI to manipulate voices and images in political advertising to do nothing. If a candidate or issue campaign used AI to create an ad, the public has a right to know,” she said.

The FCC disclosure proposal strayed onto the turf of the more business-friendly, Federal Election Commission (FEC). The FEC objected to the competition from the FCC, and though later resolved, the spat slowed the rulemaking process and the FCC rule has yet to be finalized.

Still, businesses should take note, Rothaus said.

Though not finalized, the FCC’s proposed disclosure rule, together with the FCC robocall AI rule, and the many state laws, signal to advertisers and other businesses, whether linked to politics or not, that they need to be extra careful when using or handling AI-generated content.

“For advertisers, this means a shift toward more of a focus on disclosure, whether in a political ad or in consumer products,” said Samantha Rothaus, partner in Davis+Gilbert’s advertising and marketing practice.

Regulators are clear that if advertisers depict a product in a way that is not authentic or make claims that aren’t supported in reality, the question of materiality comes into play, she said.

Similarly, advertisers who use AI to generate something about an opposing candidate that is not true, also is material, Rothaus said.

“It’s misleading whether it’s done with Photoshop or AI. It’s kind of like the means to an end doesn’t matter,” Rothaus said.

Corradino doesn’t have clients in political advertising but if she did, her advice wouldn’t be any different from what she tells all advertisers, including what might require disclosure and what would need to be substantiated when making claims about a candidate.

There is a general lack of specificity in the regulations about when disclosure must be made, especially when AI is used more subtly, Rothaus said.

For example, if AI is used to clean up the audio to translate an ad into a language other than English, does that need to be disclosed?

“Or is it an incidental use that a consumer doesn’t care about? I haven’t seen clear guidance on this yet by a regulatory body,” Rothaus said.

Of course, FCC regulations have a limited reach and likely wouldn't touch foreign bad actors, Nick Espinosa, chief security fanatic at Security Fanatics, said following his presentation at Compliance Week's AI Summit in October.

"If I'm sitting in Russia or China, what's the FCC going to do, arrest me in China?"

RATE THIS RESOURCE

Select your rating



MORE FROM ADRIANNE APPEL >>



Vystar pays \$1.5 million for alleged lack of due diligence with launch of troubled banking system



FCC teams up with CPPA to enforce privacy rules



AI & Compliance Summit: Regs discuss artificial intelligence guardrails for financial services