R Street

Free markets. Real solutions.

August 2024

R Sheet On
AI and Elections

Background

Artificial intelligence (AI) is rapidly integrating into all aspects of modern society—a trend that will accelerate as the technology continues to advance and costs decline. While experts have not yet settled on a single definition of AI, one succinct version is "the capability of computer systems or algorithms to imitate intelligent human behavior." In the context of elections, AI is a tool that can generate positive or negative impacts across three distinct aspects of the American electoral ecosystem: (1) administration, (2) cybersecurity, and (3) the information environment.

Much of the public dialogue around AI and elections has centered on potential harms to the information environment driven by the enhanced capabilities to deceive voters via deepfakes and other forms of misinformation and disinformation. In response, government officials in Washington, D.C. and state capitals have scrambled to craft rules and regulations that attempt to crack down on these harmful uses of AI technology. In fact, over the past two years, 16 states have approved new laws regulating AI deepfakes, and federal agencies are considering how new and existing regulations can apply to AI. At the same time, local election officials are exploring how AI can be used to increase operational efficiency, and cybersecurity professionals are preparing to defend election infrastructure against enhanced AI-driven cyberattacks.

Because AI presents a wide range of election risks and opportunities, lawmakers must craft policies that take reasonable steps to minimize risk without suppressing free speech or the significant benefits AI can deliver.

Current Debate

The 2024 election cycle is the first to occur in America under enhanced AI conditions. The uncertainty around the real-world impacts of AI drives disagreement on the perceived risk and the appropriate response by election administrations and policymakers.

ELECTION ADMINISTRATION: AI holds great promise as a productivity tool for the more than 10,000 local election jurisdictions across the country. It can be used to streamline administrative tasks like proofreading ballots before they are printed, assist with fulfilling public records requests, and eventually help with more complex tasks like verifying voter signatures or analyzing stray marks on hand-marked paper ballots.

On the other hand, AI is not wholly accurate, so an overreliance on the technology could result in errors that undermine public confidence in the election process. Advocates for a more restrained use of AI are especially concerned about AI's role in making judgment calls that impact an individual's ability to cast a ballot and in using AI chatbots, which can deliver erroneous information.

CYBERSECURITY: Cyberattacks on election infrastructure are long-standing concerns, and AI provides enhanced capabilities to disrupt election offices through sophisticated data breaches that expose confidential information or distributed denial of service attacks on election office websites that prevent public access to important information about voting times and locations. These attacks can be especially damaging when paired with disinformation campaigns that amplify perceived consequences of even minor cyber incidents.

At the same time, AI can bolster cyber defenses by enhancing threat detection and remediation. In addition, existing cybersecurity best practices like multifactor authentication, strong passwords, email authentication protocols, and cybersecurity training still provide important protection against sophisticated AI-generated threats.

Summary

- **AI is a powerful tool that can be used to generate positive or negative impacts across election administration, cybersecurity, and the information environment.**
- **The potential harm of AI-generated disinformation is driving the government policy response, with 18 states now restricting the use of deceptive AI-generated election communications in some manner.**
- **AI has beneficial applications in election administration and cybersecurity, and attempts to regulate AI-generated election information could violate the First Amendment.**
- **AI technology is here to stay, and government officials should encourage the productive use of AI in election administration, cybersecurity, and the information environment while countering potential harms and protecting free speech.**

INFORMATION ENVIRONMENT: AI tools allow users to easily generate high-quality false images, audio, and video at low cost. While the impact of this technology remains unclear, 18 states have stepped in with rules and regulations that aim to protect voters from deceptive information by requiring labels or imposing outright bans on AI-generated false information.

Opponents of this regulatory approach point to First Amendment concerns around restricting political speech. In fact, an appeals court in Texas ruled that a ban on AI-generated deepfakes that lawmakers approved in 2019 violated the First Amendment. And while the U.S. Supreme Court has authorized disclosure requirements in a federal campaign finance context, it remains unclear how they would view this new batch of requirements related to AI-generated speech.

Eighteen states have stepped in with rules and regulations that aim to protect voters from deceptive information by requiring labels or imposing outright bans on AI-generated false information.

Action Items

AI technology is here to stay, and government officials and other election stakeholders can take specific actions to encourage the productive use of AI in election administration, cybersecurity, and the information environment while countering potential harms and protecting free speech.

Action Items for Adapting to Increased Use of AI in Elections

Administration	• Responsibly and transparently incorporate AI into office operations by maintaining human touchpoints and communicating with the public about how AI is used. • Leverage federal security funds to experiment with strategies for countering election disinformation through proactive communications about voting times and locations. • Develop contingency plans and conduct tabletop exercises to practice responses to AI-driven disruptions before Election Day.
Cybersecurity	• Utilize cyber hygiene vulnerability-scanning services and request in-person cybersecurity assessment from the Cyber Infrastructure Security Agency. • Ensure that long-standing cybersecurity best practices like multifactor authentication, strong passwords, and cybersecurity training are in place.
Information Environment	• Voters should remain skeptical of information consumed online, consult multiple sources to verify information, resist emotional manipulation, and take personal responsibility for not spreading false information. • State and local election officials should build trust with the public to remain a source of credible election information. • Media, civil society organizations, and private-sector technology companies should support voter education and drive public awareness campaigns about AI disinformation risks.

The 2024 election will take place across thousands of diverse jurisdictions that have responded to AI risks in different ways. As noted above, election-related deepfakes will be subject to some form of regulation in 18 states but will be unregulated in the rest. This will result in a natural experiment that can inform future AI policy decisions for states based on what actually occurs.

Contact Us

For more information on this subject, contact:
R Street Institute
1411 K St. NW Ste 900,
Washington, D.C. 20005
(202) 525-5717
www.rstreet.org

Chris McIsaac
Fellow
Governance
(508) 776-0725
cmcisaac@rstreet.org

Matt Germer
Policy Director
Governance
(714) 609-6288
mgermer@rstreet.org