Impact of Artificial Intelligence on Elections

By Chris McIsaac

This paper explores AI impacts on the election information environment, cybersecurity, and election administration to define and assess risks and opportunities.

Table of Contents

Executive Summary

Artificial intelligence (AI) is already having an impact on upcoming U.S. elections and other political races around the globe. Much of the public dialogue focuses on AI's ability to generate and distribute false information, and government officials are responding by proposing rules and regulations aimed at limiting the technology's potentially negative effects. However, questions remain regarding the constitutionality of these laws, their effectiveness at limiting the impact of election disinformation, and the opportunities the use of AI presents, such as bolstering cybersecurity and improving the efficiency of election administration. While Americans are largely in favor of the government taking action around AI, there is no guarantee that restrictions will curb potential threats.

This paper explores AI impacts on the election information environment, cybersecurity, and election administration to define and assess risks and opportunities. It also evaluates the government's AI-oriented policy responses to date and assesses the effectiveness of primarily focusing on regulating the use of AI in campaign communications through prohibitions or disclosures. It concludes by offering alternative approaches to increased government-imposed limits, which could

empower local election officials to focus on strengthening cyber defenses, build trust with the public as a credible source of election information, and educate voters on the risk of AI-generated disinformation and how to recognize it.

AI technology is here to stay, so it is incumbent that our leaders and citizens adapt to its use without seeking protection via government rules and regulations that are unlikely to achieve their intended purpose.

Introduction

As the technology continues to advance and integrate into all aspects of modern society, AI is already garnering attention for impacting elections around the globe.[1] To date, much of the public dialogue has focused on AI as a threat because of its potential to accelerate the creation and distribution of disinformation and deepfakes.[2] Unsurprisingly, government officials are responding to these concerns by proposing or enacting rules and regulations aimed at limiting AI's potential negative effects.[3] Similarly, technology companies are outlining detailed agendas for how they plan to mitigate harm from deceptive AI election content.[4]

Importantly, however, AI also holds the potential to bolster the security of an election's cyber infrastructure and improve the efficiency of election administration.[5] Therefore, rather than proposing additional limits on AI-generated speech, which may run afoul of the First Amendment and would likely do little to curb any threats posed by the technology, federal and state policymakers should empower local election officials to focus on strengthening cyber defenses, build trust with the public as a credible source of election information, and educate voters on the risk of AI-generated disinformation and how to recognize it.

In this paper, we explore the range of AI impacts on elections, both positive and negative, and document the types of policy responses that have been put forward by federal and state government officials. In doing so, we discuss some of the challenges policymakers face in achieving stated policy goals. We finish by discussing the essential role that individual voters, election officials, and candidates need to play in minimizing the potential harms of AI while maximizing its benefits. Ultimately, AI technology is here to stay, and it is vital that our leaders and individual citizens take on the responsibility of adapting to this new reality while setting aside the temptation to seek protection from government rules and regulations that are unlikely to achieve their intended purpose.

AI also holds the potential to bolster the security of an election's cyber infrastructure and improve the efficiency of election administration.

1. John Peabody, "The AI Election Threat is Significant, Not Insurmountable," Aspen Institute, April 2, 2024. https://www.aspeninstitute.org/blog-posts/the-ai-election-threat-is-significant-not-insurmountable.
2. Chelsey Cox, "'Watch out': Senate Intelligence chair cautions on AI 'deep fakes' ahead of 2024 election," CNBC, Sept. 20, 2023. https://www.cnbc.com/2023/09/20/ai-could-harm-2024-us-election-senate-intelligence-chair-warns.html; Ali Swenson and Christine Fernando, "As social media guardrails fade and AI deepfakes go mainstream, experts warn of impact on elections," *Associated Press*, Dec. 26, 2023. https://apnews.com/article/election-2024-misinformation-ai-social-media-trump-6119ee6f498db10603b3664e9ad3e87e; Mark Scott, "Deepfakes, distrust and disinformation: Welcome to the AI election," *Politico*, April 16, 2024. https://www.politico.eu/article/deepfakes-distrust-disinformation-welcome-ai-election-2024.
3. Sophia Fox-Sowell, "How state lawmakers, election officials are fighting AI deepfakes," StateScoop, March 25, 2024. https://statescoop.com/deepfakes-presidential-election-ai-2024.
4. Matt O'Brien and Ali Swenson, "Tech companies sign accord to combat AI-generated election trickery," *Associated Press*, Feb. 16, 2024. https://apnews.com/article/ai-generated-election-deepfakes-munich-accord-meta-google-microsoft-tiktok-x-c40924ffc68c94fac74fa994c520fc06.
5. Haiman Wong et al., "The Transformative Role of AI in Cybersecurity: Understanding Current Applications and Benefits," R Street Institute, Jan. 24, 2024. https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-understanding-current-applications-and-benefits; Norman Eisen et al., "8 best practices for state election officials on AI," The Brookings Institution, March 11, 2024. https://www.brookings.edu/articles/8-best-practices-for-state-election-officials-on-ai.

Overview: Artificial Intelligence and Elections

AI refers to the "capability of computer systems or algorithms to imitate intelligent human behavior."[6] The term dates back to the 1950s, and AI capabilities have grown alongside improvements in computing overall. In recent years, AI sophistication has accelerated rapidly while the costs associated with accessing it have declined.[7]

AI is already integrated into many aspects of the U.S. economy, and many people interact with AI tools in their daily life. For example, banks use AI to assist in a variety of functions including fraud protection and credit underwriting.[8] Email services like Gmail utilize AI to block unwanted spam messages, and ecommerce websites like Amazon use AI to connect individual shoppers with the products they are seeking.[9] Yet, despite its existing integration in the background of modern life, AI recently entered the public consciousness in a more direct way with the release of OpenAI's ChatGPT, a chatbot that can create written content and produce highly realistic audio recordings, photos, and videos using "generative AI" tools.[10] When AI is used to imitate well-known people, particularly for nefarious purposes, the result is known as a "deepfake."

From an election perspective, these advances in AI technology are likely to impact the overall information environment, cybersecurity, and administrative processes. Although this emerging technology has garnered attention largely for its risks, as we outline below, there are also significant potential benefits to leveraging AI in our election environment.

Information Environment

An election's information environment is the most obvious area in which AI could have a potential impact.[11] AI tools can empower users to generate and distribute false information quickly, convincingly, and at a very low cost. The information itself can range from sophisticated deepfake videos created through generative AI programs to simpler text- or image-based disinformation.[12]

In terms of distribution, AI tools can enable bots to flood social media sites with an overwhelming wave of misinformation.[13] AI technology can also be paired with other communication methods such as cell phones to create and deliver targeted deceptive robocalls.[14] This misinformation could be technical, such as lies about changes to voter eligibility or the return deadline for absentee ballots, or political, such as a video of a candidate speech that never actually happened.

AI tools can empower users to generate and distribute false information quickly, convincingly, and at a very low cost.

6. "Artificial Intelligence," Merriam-Webster, last accessed April 11, 2024. https://www.merriam-webster.com/dictionary/artificial%20intelligence.
7. Rockwell Anyoha, "The History of Artificial Intelligence," Science in the News, Aug. 28, 2017. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence.
8. Miriam Fernández, "AI in Banking: AI Will Be An Incremental Game Changer," S&P Global, Oct. 31, 2023. https://www.spglobal.com/en/research-insights/featured special-editorial/ai-in-banking-ai-will-be-an-incremental-game-changer.
9. Bernard Marr, "The 10 Best Examples Of How AI Is Already Used In Our Everyday Life," *Forbes*, Dec. 16, 2019. https://www.forbes.com/sites bernardmarr/2019/12/16/the-10-best-examples-of-how-ai-is-already-used-in-our-everyday-life/?sh=659bda611171.
10. Kim Martineau, "What is generative AI?," IBM, April 20, 2023. https://research.ibm.com/blog/what-is-generative-AI.
11. Ingrid Bicu, "The Information Environment Around Elections," International IDEA, last accessed April 11, 2024. https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections.
12. Shannon Bond, "It takes a few dollars and 8 minutes to create a deepfake. And that's only the start," NPR, March 23, 2023. https://www.npr.org/2023/03/23/1165146797/it-takes-a-few-dollars-and-8-minutes-to-create-a-deepfake-and-thats-only-the-sta.
13. Nick Hajli, "Election disinformation: how AI-powered bots work and how you can protect yourself from their influence," The Conversation, April 9, 2024. https://theconversation.com/election-disinformation-how-ai-powered-bots-work-and-how-you-can-protect-yourself-from-their-influence-227174.
14. Ali Swenson, "AI-generated voices in robocalls can deceive voters. The FCC just made them illegal," *Associated Press*, Feb. 8, 2024. https://apnews.com/article/fcc-elections-artificial-intelligence-robocalls-regulations-a8292b1371b3764916461f60660b93e6.

Such AI-generated misinformation has already entered our political sphere. During the lead-up to the 2024 New Hampshire Democratic primary, many voters received a robocall message discouraging them to vote from a voice that sounded like it belonged to President Joe Biden.[15] However, investigators determined that the audio recording was generated by AI and commissioned by a supporter of Dean Phillips, one of Biden's opponents in the primary election.[16]

On the Republican side, a Super PAC supporting Ron DeSantis for president ran a television advertisement featuring language written by Donald Trump in a social media post and read by a voice that sounded like Trump but was generated by AI.[17] Unlike the Biden robocall, the message in the ad accurately represented something communicated by Trump, but the audience was still left with the false impression that Trump had made the statement in a recorded speech.

While each of these examples were quickly identified as deepfakes and were deconstructed extensively in the media, they function as a harbinger of future deceptive campaign tactics, particularly in lower-profile races with fewer resources and dimmer media spotlights. Even in high profile races with narrow margins, the use of such deceptive tactics in a key swing state could have a significant impact, especially considering that false information spreads quickly on social media.[18]

Current responses to this threat are multipronged. In the private sector, major tech companies released an agreement in February 2024 outlining their approach to managing the threat of deceptive AI related to elections.[19] The accord emphasizes voluntary measures to identify and label deceptive AI content and supports efforts to educate the public about AI risks.[20] At the same time, individual companies have taken steps to limit the use of their products or platforms for political purposes altogether.[21]

Meanwhile in the public sector, federal and state lawmakers have introduced new bills and regulations to prohibit or require greater public disclosure when AI is used in political communications. State and local election officials have also mobilized across the country by holding tabletop exercises to practice their responses to various potential disruptions, including AI-generated misinformation.[22]
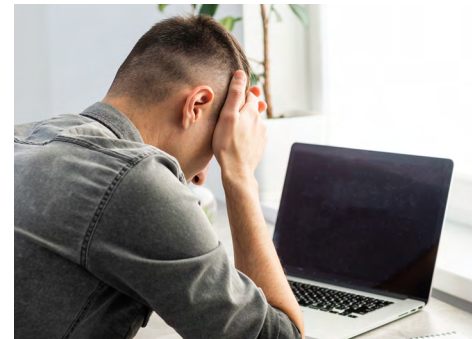
Even in high profile races with narrow margins, the use of such deceptive tactics in a key swing state could have a significant impact, especially considering that false information spreads quickly on social media.

15. Alex Seitz-Wald and Mike Memoli, "Fake Joe Biden robocall tells New Hampshire Democrats not to vote Tuesday," NBC News, Jan. 22, 2024. https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984.

16. Holly Ramer and Kevin McGill, "Magician says political consultant hired him to create AI robocall ahead of New Hampshire primary," *Associated Press*, Feb. 23, 2024. https://apnews.com/article/biden-robocalls-ai-magician-new-hampshire-louisiana-155b3ffe9d24048f3380104f95b48a57.

17. Miranda Nazzaro, "Pro-DeSantis group uses AI version of Trump's voice in new ad," *The Hill*, July 18, 2023. https://thehill.com/homenews/campaign/4103157-pro-desantis-group-uses-ai-version-of-trumps-voice-in-new-ad.

18. Peter Dizikes, "Study: On Twitter, false news travels faster than true stories," MIT News, March 8, 2018. https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

19. "A Tech Accord to Combat Deceptive Use of AI in 2024 Elections," AI Elections accord, last accessed April 11, 2024. https://www.aielectionsaccord.com/uploads/2024/02/A-Tech-Accord-to-Combat-Deceptive-Use-of-AI-in-2024-Elections.FINAL_.pdf.

20. Tiffany Hsu and Cade Metz, "In Big Election Year, A.I.'s Architects Move Against Its Misuse," *The New York Times*, Feb. 16, 2024. https://www.nytimes.com/2024/02/16/technology/ai-elections-defense.html.

21. Katie Paul, "Meta bars political advertisers from using generative AI ads tools," *Reuters*, Nov. 7, 2023. https://www.reuters.com/technology/meta-bar-political-advertisers-using-generative-ai-ads-tools-2023-11-06. "How OpenAI is approaching 2024 worldwide elections," OpenAI, Jan. 15, 2024. https://openai.com/blog/how-openai-is-approaching-2024-worldwide-elections.

22. Derek B. Johnson, "Training days: How officials are using AI to prepare election workers for voting chaos," Cyberscoop, March 14, 2024. https://cyberscoop.com/ai-election-wokers-training-deepfakes.

Cybersecurity

Cyberattacks, which seek to steal confidential information, change information within a system, or shut down the use of a system, have been a longstanding risk to elections. For example, a cyberattack on a voter registration database could increase the risk of identity theft or prevent the timely reporting of results if an election office website is taken offline. Cyberattacks can also be paired with coordinated disinformation campaigns to amplify the consequences of a minor cyber incident to damage public perception around the integrity of the election.[23]

Recognizing this risk, the federal government designated elections as "critical infrastructure" in 2017 and, in 2018, tasked the Cybersecurity and Infrastructure Security Agency (CISA) with oversight of the nation's election cybersecurity.[24] While cyberattacks, particularly from overseas actors, continue to remain a pressing threat, CISA has recognized that "generative AI capabilities will likely not introduce new risks, but they may amplify existing risks to election infrastructure."[25]

For example, efforts to access confidential data often include attacks on voter registration databases that contain personally identifiable information such as names, birthdates, addresses, driver's license numbers, and partial social security numbers. In 2016, hackers gained access to voter registration databases in Arizona through a phishing email to a Secretary of State's office staffer and in Illinois through a structured query language (SQL) injection—a common technique used to take malicious action against a database through a website.[26] More recently in Washington, D.C., hackers stole voter data and offered it for sale online in October 2023.[27] Similarly, 58,000 voters from Hillsborough County, Florida, had their personal information exposed after an unauthorized user copied files containing voter registration data.[28]

Beyond the theft of personal information, cyber-criminals can disrupt access to a system or website through a distributed denial of service (DDOS) attack. These attacks commonly seek to overwhelm a website, ultimately shutting the website down, by generating high volumes of traffic through the use of bots working in tandem.[29] The Mississippi Secretary of State's site suffered a DDOS attack on election day in 2022, which prevented public access to the website. While DDOS attacks disrupt the flow of information, they are relatively limited in impact and generally do not affect the voting process or ballot integrity.[30]

While DDOS attacks disrupt the flow of information, they are relatively limited in impact and generally do not affect the voting process or ballot integrity.

23. Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Cyber Risk Assessment," U.S. Department of Homeland Security, July 29, 2020, pp. 3-5. https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf#page=3.

24. Office of the Press Secretary, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," U.S. Department of Homeland Security, Jan. 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

25. Cyber Security and Infrastructure Security Agency, "Risk in Focus: Generative A.I. and the 2024 Election Cycle," U.S. Department of Homeland Security, Jan. 18, 2024, p. 1. https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf.

26. Testimony of Steve Sandvoss, U.S. Senate Select Committee on Intelligence, "Illinois Voter Registration System Database Breach Report," 115th Congress, June 21, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-ssandvoss-062117_0.pdf; Matt Hunter, "Email that hacked AZ voter registration looked like an employee, official says," CNBC, Oct. 5, 2016. https://www.cnbc.com/2016/10/05/email-that-hacked-az-voter-registration-looked-like-an-employee-said-official.html.

27. Caroline Nihill, "DC Board of Elections breach may include entire voter roll," Cyberscoop, Oct. 23, 2023. https://cyberscoop.com/dc-board-elections-breach.

28. Leilyn Torres, "Illegal data breach affects about 58,000 voters in Hillsborough, Supervisor of Elections says," WFTS Tampa Bay, May 31, 2023. https://www.abcactionnews.com/news/region-hillsborough/illegal-data-breach-affects-about-58-000-voters-in-hillsborough-supervisor-of-elections-says.

29. Cyber Security and Infrastructure Security Agency, "No Downtime in Elections: A Guide to Mitigating Risks of Denial-of-Service," U.S. Department of Homeland Security, September 2023, p. 1. https://www.cisa.gov/sites/default/files/2023-09/Mitigating_DoS_to_Election_Infrastructure_V2_508c.pdf.

30. Mark Albert, "Cyberattack against Mississippi secretary of state's website under investigation," WAPT Jackson, Nov. 9, 2022. https://www.wapt.com/article/cyberattack-launched-against-mississippi-secretary-of-states-website-cisa-says/41904312.

Although it is clear that AI has accelerated the sophistication and power of cyberattacks, it is important to recognize that it can also bolster our cyber defenses. The technology can help improve threat detection and remediation, enhance efficiency of the cyber workforce by handling more routine tasks, and strengthen data security.[31] While it may be easier for many election officials to identify the threats raised by emerging technologies like AI, they must also look for appropriate ways to incorporate AI into their cybersecurity strategies.

Even if election offices start to incorporate AI into their cyber defense, a number of existing cybersecurity best practices can help reduce the threat of AI attacks. Multifactor authentication, strong passwords, email authentication protocols, and cybersecurity training for staff can help stop AI-generated phishing and social engineering attacks. According to CISA, "election officials have the power to mitigate against these risks heading into 2024, and many of these mitigations are the same security best practices experts have recommended for years."[32]

Election Administration

One of the hallmarks of the election system in America is decentralization. Elections are administered at the state and local level, with more than 10,000 election jurisdictions across the country.[33] This design can instill confidence in the process by maintaining a sense of connection between voters and the individuals administering their local election while making it more difficult for bad actors to disrupt elections at scale. At the same time, this approach can also have operational inefficiencies and workforce challenges, some of which could be improved through tools employing AI technology.

One example of where AI could help election administrators is in the tabulation of hand-marked paper ballots. Approximately 95 percent of U.S. voters will cast a paper ballot in 2024, and most of those votes will be cast by filling in a bubble or checking a box with a pen.[34] The rest will use ballot-marking devices where the voter makes the selections on a machine that then generates a paper ballot with the voter's choices. Both types of paper ballots are then processed through an optical scanner that records the votes.[35]

Invariably, a certain number of hand-marked ballots will be unreadable by the optical scanner for some reason, ranging from physical damage to unclear markings.[36] When this happens, the ballot must be reviewed by election workers and either replicated on a new readable ballot or hand counted, depending on the jurisdiction.[37]

Best Practices:

Multifactor authentication

Strong passwords

Email authentication protocols

Cybersecurity training

31. Wong et al. https://www.rstreet.org/commentary/the-transformative-role-of-ai-in-cybersecurity-understanding-current-applications-and-benefits.

32. Cyber Security and Infrastructure Security Agency, "Risk in Focus: Generative A.I. and the 2024 Election Cycle," pp. 1-2. https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf.

33. "Election Administration at State and Local Levels," National Conference of State Legislatures, Dec. 22, 2023. https://www.ncsl.org/elections-and-campaigns/election-administration-at-state-and-local-levels.

34. "The Verifier — Election Day Equipment — November 2024," Verified Voting, last accessed April 16, 2024. https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024.

35. "Voting Equipment," Verified Voting, last accessed April 16, 2024. https://verifiedvoting.org/votingequipment.

36. "Ballot Replication Guide," The Elections Group, Oct. 5, 2022. https://electionsgroup.com/resource/ballot-replication-guide.

37. "Ballot Duplication," National Conference of State Legislatures, Aug. 1, 2023. https://www.ncsl.org/elections-and-campaigns/ballot-duplication.

R Street

Free markets. Real solutions.

Impact of Artificial Intelligence
on Elections

R Street Policy Study
No. 304

June 2024

Researchers from three universities are developing a system that uses AI to assist in this process of reviewing hand-marked paper ballots.[38] Specifically, the technology would serve as a check on the primary ballot scanner by identifying ballots for election workers to analyze more closely due to ballot anomalies such as marks outside the typical voting area or bubbles that are lightly filled in. They are also exploring how the technology could help identify fraudulent ballots completed by a single individual.[39]

Signature verification is another process where AI is already helping improve the efficiency of election administration. To confirm that a ballot belongs to the intended voter, many states require signature verification for mail-in ballots, which involves comparing the on-file signature of an individual to the signature on the envelope containing the ballot.[40] This is a time-consuming and labor-intensive process that can be expedited with the assistance of technology that identifies signatures that require additional human review. As of 2020, there were at least 29 counties using AI for this purpose.[41]

An important consideration for the use of AI in these types of election-administration tasks is to maintain human touchpoints throughout the process.[42] AI tools are not perfect, so humans must be involved, especially when AI is used to help determine a voter's eligibility to cast a ballot or whether a mail-in ballot will be counted based on the signature verification. It will also be important for election offices to be transparent with the public about the vendor, how the tool is used, and any plans for addressing problems that arise.[43]

Public record requests provide a final example of AI deployment in election administration, and they succinctly illustrates both the potential risks and benefits of the technology. Since 2020, election offices have experienced an uptick in public record requests.[44] While there are certainly legitimate reasons for seeking access to public documents and encouraging government transparency, there are also ample opportunities to make records requests in bad faith as a way of bogging down the system. Unfortunately, AI could be used to worsen the problem. A bad actor could use AI tools to rapidly generate and disseminate requests across multiple jurisdictions to divert resources in understaffed election offices and disrupt election processes.[45]

Yet, in the same stroke, AI helps increase transparency while keeping local election officials focused on running elections. Local officials can use AI to process records requests and initiate the search for relevant records, ultimately leading to an overall increase in government efficiency and transparency. A number of federal agencies—including the State Department, Justice Department, and Centers for Disease Control and Prevention—are already experimenting with using AI tools to assist in managing and fulfilling public-

AI tools are not perfect, so humans must be involved, especially when AI is used to help determine a voter's eligibility to cast a ballot or whether a mail-in ballot will be counted based on the signature verification.

38. "On the bubble: Artificial intelligence could help elections count hand-marked ballots with greater speed and accuracy," Texas A&M University, Sept. 2, 2022. https://research.tamu.edu/2022/09/02/on-the-bubble-artificial-intelligence-could-help-elections-count-hard-marked-ballots-with-greater-speed-and-accuracy/.

39. "Award Abstract # 2154589 Collaborative Research: SaTC: CORE: Medium: Bubble Aid: Assistive AI to Improve the Robustness and Security of Reading Hand-Marked Ballots," U.S. National Science Foundation, last accessed April 11, 2024. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2154589&HistoricalAwards=false.

40. "Table 14: How States Verify Voted Absentee/Mail Ballots," National Conference of State Legislatures, Jan. 22, 2024. https://www.ncsl.org/elections-and-campaigns/table-14-how-states-verify-voted-absentee-mail-ballots.

41. Paresh Dave and Andy Sullivan, "Factbox: U.S. counties using automated signature verification software," *Reuters*, Sept. 24 2020. https://www.reuters.com/article/us-usa-election-ballot-signatures-softwa/factbox-u-s-counties-using-automated-signature-verification-software-idUSKCN26F1U4.

42. Eisen et al. https://www.brookings.edu/articles/8-best-practices-for-state-election-officials-on-ai.

43. Edgardo Cortés et al., "Safeguards for Using Artificial Intelligence in Election Administration," Brennan Center for Justice, Dec. 12, 2023. https://www.brennancenter.org/our-work/research-reports/safeguards-using-artificial-intelligence-election-administration.

44. "Best Practices: Public Records Requests," U.S. Election Assistance Commission, March 2023, p. 2. https://www.eac.gov/sites/default/files/electionofficials/Public_Records_Requests_Best_Practices_508.pdf.

45. Meredith Moran, "Misinformation, frivolous record requests bog down election offices," National Association of Counties, Oct. 10, 2022. https://www.naco.org/articles/misinformation-frivolous-record-requests-bog-down-election-offices.

record requests.[46] Local election offices could benefit from similar AI tools to help manage the influx of requests while maintaining focus on their primary function of administering secure and trustworthy elections.

Policy Responses

In response to advancing AI technology, policymakers at the federal and state level are primarily focused on minimizing the impact of AI-driven election disinformation.[47] The proposals they draft often seek to prohibit the use of AI for deceptive purposes in elections or require disclosure of the use of AI in campaign speech.[48]

At the federal level, members of Congress have introduced at least five bills aimed at restricting AI in elections and two of these were approved by the Senate Rules committee on May 15.[49] Independent agencies like the Federal Communications Commission (FCC) and Federal Elections Commission (FEC) have also taken or are considering action under their existing regulatory authority.[50] Meanwhile, 17 states now have laws on the books that ban the use of AI in certain election circumstances or establish disclosure requirements.[51]

These legislative moves indicate that there is clearly momentum in favor of continued government action around AI. Public opinion is generally in favor of these actions across party lines.[52] However, questions remain regarding the constitutionality of these laws, as well as their effectiveness at limiting the impact of election disinformation. In the following section, we examine these efforts to minimize AI-driven electoral harms through legislation and regulation that establishes disclosure requirements and prohibitions. We also assess how a less restrictive legislative proposal in Congress and a recent decision by the U.S. Election Assistance Commission (EAC) could provide lessons for an alternative approach that empowers local election officials and emphasizes public education and individual responsibility.

Prohibition and Disclosure

In response to the potential impacts of AI on elections, policymakers have generally proposed or enacted laws and regulations that either ban the use of AI for certain purposes or require a disclosure indicating that AI was used to produce the image, video, or audio used in the election communication. Among the states that have enacted legislation related to AI and elections, requiring a disclosure is the most common approach.

17 states now have laws on the books that ban the use of AI in certain election circumstances or establish disclosure requirements.

46. Lewis Kamb, "Some U.S. government agencies are testing out AI to help fulfill public records requests," *NBC News*, Aug. 1, 2023. https://www.nbcnews.com/news/us-news/federal-agencies-testing-ai-foia-concerns-rcna97313.

47. Steve Collins, "U.S. Senate Weighs Restricting AI Use in Elections," Government Technology, Oct. 2, 2023. https://www.govtech.com/policy/u-s-senate-weighs-restricting-ai-use-in-elections; Zachary Roth, "States rush to combat AI threat in elections," Stateline, March 28, 2024. https://stateline.org/2024/03/28/states-rush-to-combat-ai-threat-to-elections.

48. Adam Edelman, "States turn their attention to regulating AI and deepfakes as 2024 kicks off," *NBC News*, Jan. 22, 2024. https://www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122.

49. "AI Legislation Tracker," American Action Forum, last accessed April 16, 2024. https://www.americanactionforum.org/list-of-proposed-ai-bills-table/?gad_source=1&gclid=CjwKCAjwh4-wBhB3EiwAeJsppMrPcaPFtrItaEjyleo8dpXRrQ5Hs9ZK6fUiC9Y5Ijh5jFOJ-Z4pExoCbIoQAvD_BwE.

50. Ali Swenson, "FEC moves toward potentially regulating AI deepfakes in campaign ads," Associated Press, Aug. 10, 2023. https://apnews.com/article/fec-artificial-intelligence-deepfakes-election-2024-95399e640bd1e41182f6c631717cc826.

51. "Artificial Intelligence (AI) in Elections and Campaigns," National Conference of State Legislatures, April 1, 2024. https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns.

52. "There Is Bipartisan Concern About the Use of AI in the 2024 Elections," The Associated Press-NORC Center for Public Affairs Research, November 2023, pp. 11-12. https://apnorc.org/wp-content/uploads/2023/11/Harris-AI-report-TO-DTP-1101_formatted.pdf#page=11.

Impact of Artificial Intelligence on Elections

## Figure 1: Legislation Enacted on Elections and AI by Type and Penalty (2019-2024)
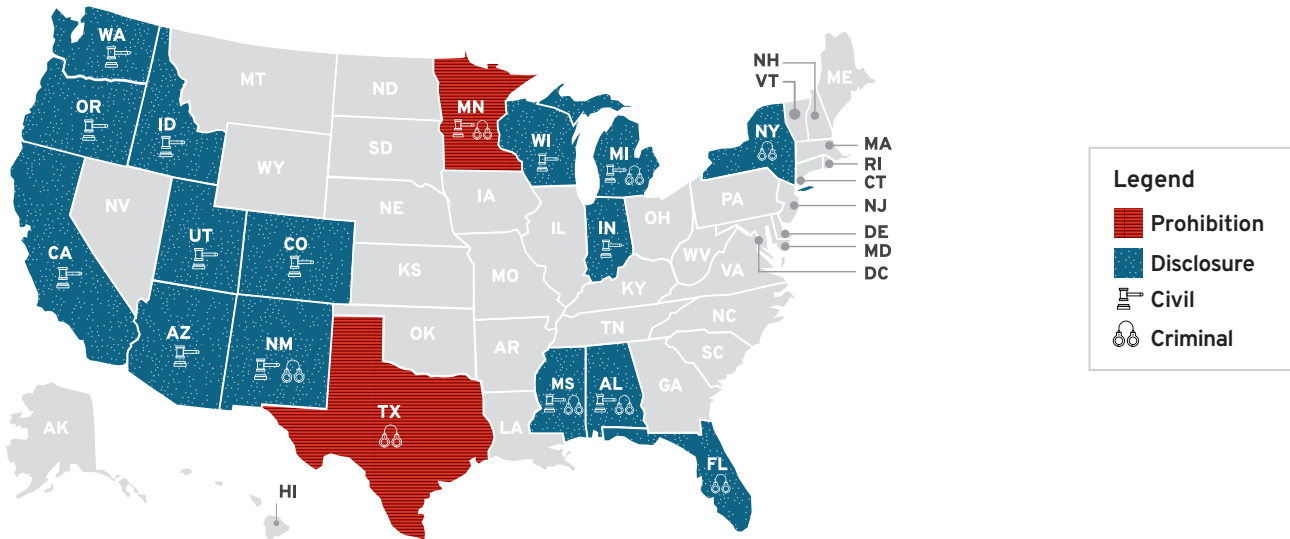
Note: Map current as of June 3, 2024.

Source: "Artificial Intelligence (AI) in Elections and Campaigns," National Conference of State Legislatures, June 3, 2024. https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns.

In Washington D.C., Congress and federal agencies are also considering new laws and regulations related to AI and elections, including a mix of prohibitions and disclosure requirements. Two such proposals that have gained some traction in Congress are S. 2770 and S. 3875.[53] Sponsored by Sen. Amy Klobuchar (D-Minn.) and approved by the U.S. Senate Rules committee in May of 2024, these bills seek to minimize the impact of AI-driven election disinformation by through bans and disclosures.[54] At the agency level, the FCC was the only agency so far to fully adopt one of these policy options when it confirmed that an existing ban on deceptive robocalls also applies to AI-generated robocalls.[55]

Figure 2: Approved and Pending Federal Restrictions on Elections and AI
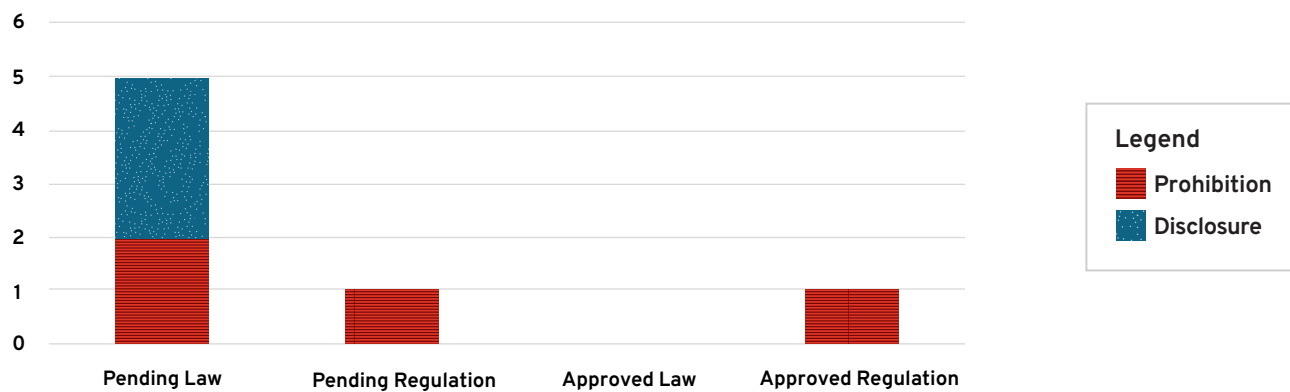
Sources: Pending laws HR 3044, HR 4611, S 1596, S 2770, S 3875. Pending Regulation is the FEC. Approved Regulation is the FCC. "AI Legislation Tracker," American Action Forum, last accessed April 16, 2024. https://www.americanactionforum.org/list-of-proposed-ai-bills-table/?gad_source=1&gclid=CjwKCAjwh4-wBhB3EiwAeJsppMrPcaPFtrItaEjyIeo8dpXRrQ5Hs9ZK6fUiC9Y5Ijh5jFOJ-Z4pExoCbIoQAvD_BwE; David Garr, "Comment sought on amending regulation to include deliberately deceptive Artificial Intelligence in campaign ads," Federal Election Commission, last accessed Aug. 16, 2023. https://www.fec.gov/updates/comments-sought-on-amending-regulation-to-include-deliberately-deceptive-artificial-intelligence-in-campaign-ads; Office of Media Relations, "FCC Makes AI Generated Voice in Robocalls Illegal," U.S. Federal Communications Commission, last accessed April 11, 2024. https://docs.fcc.gov/public/attachments/DOC-400393A1.pdf.

53. S. 2770, "Protect Elections from Deceptive AI Act," 118th Congress. https://www.congress.gov/118/bills/s2770/BILLS-118s2770is.pdf.S. 3875, "AI Transparency in Elections Act of 2024," 118th Congress. https://www.congress.gov/118/bills/s3875/BILLS-118s3875rs.pdf
54. Rebecca Klar, "Election -related AI bills test bipartisan support for regulation," The Hill, May 15, 2024. https://thehill.com/policy/technology/4666277-election-related-ai-bills-test-bipartisan-support-for-regulation/.
55. Shannon Bond, "The FCC says AI voices in robocalls are illegal," NPR, Feb. 8, 2024. https://www.npr.org/2024/02/08/1230052884/the-fcc-says-ai-voices-in-robocalls-are-illegal.

Disclosure

The most common approach to regulation is requiring a disclosure when AI is used to generate content in an election communication. Currently, 15 states have approved legislation requiring a disclosure when AI-generated election content appears in a communication, and three bills are pending in Congress that would require a similar approach, including S 3875.[56]

The disclosure requirements generally apply only if the AI-generated media is materially deceptive and/or intended to influence the outcome of the elections. In some cases, the restriction is limited to a certain time period before the election, such as 60 or 90 days.[57] These parameters narrow the application of the laws so that innocuous uses of AI are not subject to the same restrictions. In terms of enforcement, states impose a mix of civil and criminal penalties, with Michigan imposing the stiffest penalty of up to 5 years in prison for a repeat offender.[58]

The rationale for this type of approach is that the public has a right to know when election communications are incorporating AI-generated content, following a playbook that is similar to the FEC rules requiring disclaimers about the source of funding for campaign advertisements and familiar statements by federal candidates that they "approve the message."[59] In addition, state governments have their own rules about disclaimers that vary significantly across the country, ranging from highly prescriptive verbiage requirements to more general statements about the sponsor of the communication.[60]

The practical impact of these requirements remains to be seen. Candidate campaigns, political action committees, and other formal organizations are likely to comply with these restrictions as such practices are already part of their standard operating procedures for traditional campaign communications. However, bad actors who seek to confuse voters and disrupt elections are not inclined to follow the rules to begin with, so these additional restrictions are unlikely to have much effect on those groups. There is also a risk of "over labeling" due to broad definitions of what qualifies as AI, which dilutes the effectiveness of disclosures in identifying the deceptive content if a high percentage of election communications choose to utilize the disclosure out of an abundance of caution.[61]

Prohibition

While less common than requiring disclosure, another approach to regulating AI in elections is to prohibit its use under certain circumstances. For example, in 2019, Texas approved a general ban on the creation and distribution of a deepfake with the intent to injure a candidate or influence the outcome within 30 days of the election. Violations are a class A misdemeanor, which can be punished by up to one year in jail and a fine of up to $4,000.[62] In 2023, Minnesota became the second state with such a

15 states have approved legislation requiring a disclosure when AI-generated election content appears in a communication, and three bills are pending in Congress that would require a similar approach.

56. "AI Legislation Tracker." https://www.americanactionforum.org/list-of-proposed-ai-bills-table/?gad_source=1&gclid=CjwKCAjwh4-wBhB3EiwAeJsppMrPcaPFtrItaEjyIeo8dpXRrQ5Hs9ZK6fUiC9Y5Ijh5jFOJ-Z4pExoCbIoQAvD_BwE.

57. "Artificial Intelligence (AI) in Elections and Campaigns." https://www.ncsl.org/elections-and-campaigns/artificial-intelligence-ai-in-elections-and-campaigns.

58. H.B. 5144, 2023 Leg, Reg. Sess. (Mich. 2023). https://www.legislature.mi.gov/documents/2023-2024/publicact/pdf/2023-PA-0265.pdf.

59. "Campaign Finance Law: Disclosure and Disclaimer Requirements for Political Campaign Advertising," Congressional Research Service, Dec. 30, 2019, p. 2. https://crsreports.congress.gov/product/pdf/IF/IF11398.

60. "Disclaimers on Political Advertisements," National Conference of State Legislatures, March 14, 2023. https://www.ncsl.org/elections-and-campaigns/disclaimers-on-political-advertisements.

61. Ethan Bueno de Mesquita et al., "Preparing for Generative AI in the 2024 Election: Recommendations and Best Practices Based on Academic Research," University of Chicago Harris School of Public Policy and Stanford Graduate School of Business, last accessed April 11, 2024, p. 6. https://harris.uchicago.edu/files/ai_and_elections_best_practices_no_embargo.pdf#page=6.

62. Matthew Ferraro, "Texas Law Could Signal More State, Federal Deepfake Bans," JD Supra, Sept. 11, 2019. https://www.jdsupra.com/legalnews/texas-law-could-signal-more-state-37742.

ban, which applies to the 90 days leading up to the election. An initial violation is punishable by up to 90 days in jail and a fine of $1,000 and increase to five years and $10,000 for a second violation within five years of the first.[63]

Meanwhile, in Washington, D.C., federal agencies are considering how existing statutes can be applied to regulate deceptive election communications generated by AI. For example, the FEC—an independent regulatory agency responsible for administering campaign finance law in federal elections—has initiated a rulemaking that could result in AI-generated communications being regulated under an existing prohibition on "fraudulent misrepresentation of campaign authority."[64] More specifically, federal campaign finance law currently prohibits candidates and their campaigns from fraudulently misrepresenting themselves as communicating or acting on behalf of an opposing candidate regarding an issue that is damaging to that other candidate. If adopted, the rulemaking could clarify that deepfakes meet the definition of communications that are already prohibited. In addition, S. 2770 introduced legislation that would bypass the FEC and directly prohibit the distribution of materially deceptive, AI-generated media related to a federal election. [65]

The FEC process follows a ruling by the FCC in February that using AI-generated voices in robocalls is illegal.[66] This decision applies to all forms of robocall scams, including those related to elections and campaigns. While much of the media coverage surrounding the decision focused on the agency acting to "ban" or "outlaw" the use of AI in robocalls, the actual decision was a simple confirmation that existing federal regulations apply to AI-generated phone calls.[67]

Moving Forward

Americans are concerned about the impact that AI could have on elections, with around one-half of the population expecting negative consequences for election procedures and a further deterioration of campaign civility.[68] The policy actions from federal and state officials are driven in large part by this public concern. However, questions remain regarding the constitutionality of some of these laws, as well as their effectiveness at achieving the stated policy goals.

For example, laws regulating the use of AI in election communications are establishing a restriction on election speech, which raises questions around violations of the First Amendment. The level of restriction depends on whether the law establishes a ban or a disclosure requirement, and the U.S. Supreme Court has largely accepted the use of disclosures and disclaimers to inform the public about things like sources of funding for campaign advertisements.[69] On the other hand, prohibiting speech based on the technology used to create or disseminate it could be more vulnerable to a

For example, laws regulating the use of AI in election communications are establishing a restriction on election speech, which raises questions around violations of the First Amendment.

63. Caroline Cummings, "New Minnesota law regulates 'deepfakes' to curb influence on elections," CBS News Minnesota, Nov. 1, 2023. https://www.cbsnews.com/minnesota/news/new-minnesota-law-regulates-deepfakes-to-curb-influence-on-elections.

64. David Garr, "Comment sought on amending regulation to include deliberately deceptive Artificial Intelligence in campaign ads," Federal Election Commission, Aug. 16, 2023. https://www.fec.gov/updates/comments-sought-on-amending-regulation-to-include-deliberately-deceptive-artificial-intelligence-in-campaign-ads.

65. S. 2770, "Protect Elections from Deceptive AI Act," 118th Congress. https://www.congress.gov/118/bills/s2770/BILLS-118s2770is.pdf.

66. Office of Media Relations, "FCC Makes AI-Generated Voice in Robocalls Illegal," Federal Communications Commission, Feb. 8, 2024. https://docs.fcc.gov/public/attachments/DOC-400393A1.pdf.

67. Cecilia Kang, "F.C.C. Bans A.I.-Generated Robocalls," *The New York Times*, Feb. 8, 2024. https://www.nytimes.com/2024/02/08/technology/fcc-ban-ai-robocalls.html; Ryan Heath, "FCC outlaws AI voices in robocall fraud," Axios, Feb. 8, 2024. https://www.axios.com/2024/02/08/fcc-ai-robocalls-illegal; Federal Communications Commission, *Declaratory Ruling 24-17: Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts,* CG Docket No. 23-362, Feb. 8, 2024, p. 1. https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf.

68. Marc S. Jacob, "Partisan Animosity and America," Polarization Research Lab, March 31, 2024. https://prlpublic.s3.amazonaws.com/reports/March2024.html

69. "Campaign Finance Law: Disclosure and Disclaimer Requirements for Political Campaign Advertising," p. 1. https://crsreports.congress.gov/product/pdf/IF/IF11398.

![R Street logo] Free markets. Real solutions.

Impact of Artificial Intelligence
on Elections

R Street Policy Study
No. 304

June 2024

constitutional challenge.[70] In the event that these AI laws are successfully challenged, election officials and the general public should be informed and prepared. This is important, regardless, as even if the government restrictions on deceptive AI content are constitutional, there is no guarantee that they will be effective.

Consider the example of the decades-long effort by the FCC to regulate illegal, unwanted robocalls. Such calls have been illegal since 1991 when Congress passed the Telephone Consumer Protection Act (TCPA), which prohibited making calls using an "artificial or prerecorded voice" without the consent of the call recipient.[71] Over the past five years, however, Americans have received, on average, more than 50 billion robocalls per year that violate the TCPA.[72] There are various explanations for why the ban is ineffective, ranging from a lack of enforcement authority to outdated definitions.[73] Recent reforms and advances in monitoring technology have the potential to change this trajectory, but the issue remains that prohibitions imposed by the government rarely work as intended.[74]

This example is particularly relevant because the scammers have consistently found a way to evade the rules as they have evolved over the years. Considering the enhanced capabilities of AI, there is no reason to believe that bad actors seeking to disrupt election processes will be any less skilled at navigating the rules than the lower-tech robocall scammers are. As a result, Americans and local election officials should anticipate the coming wave of AI-driven disinformation and focus on preparing to identify and counter the potential impacts.

An example of this alternative approach comes from the U.S. Election Assistance Commission (EAC), a federal commission that helps election officials improve the administration of elections by serving as a national information clearinghouse, setting voluntary election equipment standards, and administering election security grants.[75] The EAC issued a decision in February confirming that certain election security grants funds they administer can be used to help local election officials counter AI-generated disinformation.[76] In comparison to the heavy-handed legislative proposals we discussed previously, the EAC's lighter touch has promise, particularly as it relates to voter education.

The main strength of the EAC approach is their emphasis on countering—rather than preventing—AI-generated election disinformation. The effectiveness will depend on the specific approach each state takes under this authority, but the most opportunity will likely be found in efforts to educate the public about accurate voting information and procedures.

Another strength of the EAC is that states have the flexibility to innovate. The EAC decision outlines allowable categories of spending, but state and local election officials are in the best position to experiment with different approaches and develop best practices for countering disinformation over time through public education.

The main strength of the EAC aproach is their empahsis on countering- rather than preventing- AI -generated election disinformation.

70. Richard Stengel, "The Case for Protecting AI-Generated Speech with the First Amendment," *Time*, May 9, 2023. https://time.com/6278220/protecting-ai-generated-speech-first-amendment.
71. 47 U.S.C. § 227(b)(1)(B). https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title47-section227&num=0&edition=prelim.
72. "Historical Robocalls By Time," YouMail Robocall Index, last accessed April 16, 2024. https://robocallindex.com/history/time.
73. Jon Brodkin, "FCC robocall enforcement does little to stop illegal calls, Senate hears," ARS Technica, Oct. 24, 2023. https://arstechnica.com/tech-policy/2023/10/many-robocallers-dont-pay-fines-as-fcc-still-lacks-legal-power-to-collect.
74. "Combatting Spoofed Robocalls with Caller ID Authentication," Federal Communications Commission, last accessed April 16, 2024. https://www.fcc.gov/call-authentication; Steven Greenhut, "We should just say 'no' to new era of Prohibition," R Street Institute, Feb. 25, 2023. https://www.rstreet.org/commentary/we-should-just-say-no-to-new-era-of-prohibition.
75. "About the EAC," United States Election Assistance Commission, last accessed April 16, 2024. https://www.eac.gov/about.
76. Paige Mellerio, "U.S. Election Assistance Commission expands use of election security funds to include countering AI-generated disinformation," National Association of Counties, Feb. 27, 2024. https://www.naco.org/news/us-election-assistance-commission-expands-use-election-security-funds-include-countering-ai.

While the most effective strategies for dealing with AI will likely emerge from outside Washington, D.C., the federal government can still play a useful role supporting local election officials. For example, in May, the Senate Rules committee approved a third bill alongside the prohibition and disclosure bills. That bill, S 3897, tasks the EAC, in consultation with the National Institute of Standards and Technology (NIST), with developing voluntary guidelines for local election officials that address the uses and risks of AI in various aspects of election administration.[77]

Voluntary guidelines are useful because they provide support to those who need the help while leaving space for individual offices to innovate and explore different strategies for adapting to this new technology. Bill S. 3987, along with the February EAC decision, creates space for this innovation while providing meaningful support to election officials as they adapt to the new reality of administering free and fair elections in the age of AI.

Public Awareness and Individual Responsibility

Despite the efforts of federal and state officials to regulate deceptive AI content, it is still likely to play a role in elections moving forward, but there are specific actions that election officials, individual citizens, and political candidates can take to limit the impact of the deception. In this section, we summarize those actions.

Election Officials

Election officials play an essential role as a source of trusted information about the voting process. They must work to establish this relationship with the public early to build the credibility necessary to counter deceptions that arise closer to Election Day. For example, last November the National Association of Secretaries of State launched an initiative to build trust with the public while individual Secretaries, such as Maggie Toulouse Oliver in New Mexico and Michael Adams in Kentucky, established online resources for countering election rumors.[78]

To support this effort, election officials should leverage the recent decision by the U.S. EAC to deploy security grant funding from the Help America Vote Act for countering election disinformation.[79] The decision by the EAC provides opportunity for innovation at the state and local level to experiment with different approaches to ensuring that the public receives accurate information about voting times, locations, and processes.

On the cybersecurity front, election officials once again play a central role in protecting the election infrastructure by ensuring that they follow best practices and take advantage of federal support from agencies like CISA. For example, election offices can sign up for CISA's free cyber hygiene vulnerability scanning services to help identify weaknesses or request an in-person cybersecurity assessment.[80]

Basic cybersecurity practices can also go a long way toward defending against sophisticated phishing and social engineering attacks strengthened by AI capabilities, such as utilizing multifactor authentication and keeping software up to date.[81]

Election officials should leverage the recent decision by the U.S. EAC to deploy security grant funding from the Help America Vote Act for countering election disinformation.

77. S. 3897, "Preparing Election Administrators for AI Act," 118th Congress. https://www.congress.gov/118/bills/s3897/BILLS-118s3897rs.pdf.

78. "#TrustedInfo2024," National Association of Secretaries of State, last accessed May 2, 2024. https://www.nass.org/initiatives/trustedinfo; "Rumor vs Reality," New Mexico Office of the Secretary State, last accessed April 11, 2024. https://www.sos.nm.gov/voting-and-elections/voter-information-portal-nmvote-org/rumor-vs-reality; "Rumor Control," Kentucky Office of the Secretary of State, last accessed May 1, 2024. https://www.sos.ky.gov/elections/Pages/Rumor-Control.aspx.

79. Chris McIsaac, "Existing Election Security Grants Can Help States Counter Election Disinformation Through Voter Education," R Street Institute, March 15, 2024. https://www.rstreet.org/commentary/existing-election-security-grants-can-help-states-counter-election-disinformation-through-voter-education.

80. Cyber Security and Infrastructure Security Agency, "Election Security Services," U.S. Department of Homeland Security, last accessed April 16, 2024. https://www.cisa.gov/topics/election-security/election-security-services.

81. Microsoft Threat Intelligence, "Basic cyber hygiene prevents 99% of attacks," Microsoft, Aug. 31, 2023. https://www.microsoft.com/en-us/security/security-insider/practical-cyber-defense/cyber-resilience-hygiene-guide.

Finally, election officials can develop contingency plans and participate in tabletop exercises to practice their response to various scenarios in advance of election day. These events allow election officials to gain experience responding to a range of disruptions and can be tailored to account for AI-driven disinformation or cyber incidents.[82]

Voters and Candidates

Voters need to remain skeptical of information they consume online and anticipate that there will likely be an uptick in deceptive content as Election Day approaches. Fortunately, voters already have a high degree of skepticism regarding election information generated by ChatGPT, so they simply need to maintain this mindset regarding information that flows to them unsolicited.[83]

One example of what this looks like in practice is a tool developed by RAND consisting of a basic three-part framework that urges individuals, when they engage with social media, to consult multiple sources, resist emotional manipulation, and take personal responsibility for not spreading false information.[84]

Civil society groups, the private sector, and media can support voter education and raise public awareness of the risks involved with AI by continuing to draw attention to the issue so that it does not slip out of the public consciousness, while also avoiding the risk of sensationalizing the issue.[85]

Finally, candidates for office have an opportunity to defuse the effects of deceptive AI-generated content by pledging to not use it and urging supporters to not use it. Candidates also need to resist the temptation to claim that unflattering audio or video is an AI deepfake when it is real. Simple decisions by leaders to avoid fanning the flames would go a long way to minimizing the potential impact of false information generated by AI.

Voters already have a high degree of skepticism regarding election information generated by ChatGPT, so they simply need to maintain this mindset regarding information that flows to them unsolicited.

Conclusion

AI has the potential to disrupt elections in 2024 and beyond with regard to election infrastructure, election cybersecurity, and election administration. The response to this threat by lawmakers has been a bipartisan rush to pass new rules and regulations aimed at limiting deceptive AI election content. Yet, instead of new rules and regulations, state and federal policymakers, as well as citizens, would be better served by empowering local election officials to focus on strengthening cyber defenses and by educating voters on the risk of AI-generated disinformation and how to recognize it. American elections are decentralized by design, and this approach, which empowers individuals at the local level, provides the best opportunity to truly strengthen American democracy for years to come.

About the Author

Chris McIsaac is a governance fellow at the R Street Institute.

82. "Arizona SOS holds first in a series of Statewide Elections Security Tabletop Exercises," Office of the Arizona Secretary of State, Dec. 19, 2023. https://azsos.gov/news/314.
83. Colleen McClain, "Americans' use of ChatGPT is ticking up, but few trust its election information," Pew Research Center, March 26, 2024. https://www.pewresearch org/short-reads/2024/03/26/americans-use-of-chatgpt-is-ticking-up-but-few-trust-its-election-information.
84. Alice Huguet et al., "Social Media Posts Have Power, and So Do You," RAND, Feb. 8, 2024. https://www.rand.org/pubs/tools/TLA2909-1.html.
85. "The AI + Election Security Coalition," last accessed on April 11, 2024. https://docsend.com/view/7f9c8rbed7bzcbp8.