POLICY REPORT

BRENNAN CENTER FOR JUSTICE

An Agenda to Strengthen U.S. Democracy in the Age of AI

By Mekela Panditharatne, Lawrence Norden, Joanna Zdanys, Daniel I. Weiner, and Yasmin Abusaif

FEBRUARY 13, 2025

Brennan Center for Justice at New York University School of Law

Table of Contents

Highlights

- >> Without proper safeguards and reforms, artificial intelligence can disenfranchise voters and amplify threats to electoral integrity.
- >> Policymakers need to minimize the dangers of AI and implement standards to improve efficiency, responsiveness, and accountability for public servants using the technology.
- >> Those who profit from AI must meet transparency requirements and be held accountable when these tools are used to undermine democratic processes.

ABOUT THE BRENNAN CENTER

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform and revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

Introduction

The year 2024 began with bold predictions about how the United States would see its first artificial intelligence (AI) election.[1] Commentators worried that generative AI — a branch of AI that can create new images, audio, video, and text — could produce deepfakes that would so inundate users of social media that they would be unable to separate truth from fiction when making voting decisions.[2] Meanwhile, some self-labeled techno-optimists proselytized how AI could revolutionize voter outreach and fundraising, thereby leveling the playing field for campaigns that otherwise could not afford expensive political consultants and staff.[3]

As the election played out, AI was employed in numerous ways: Foreign adversaries used the technology to augment their election interference by creating copycat news sites filled with what appeared to be AI-generated fake stories.[4] Campaigns leveraged deepfake technology to convincingly imitate politicians and produce misleading advertisements.[5] Activists deployed AI systems to support voter suppression efforts.[6] Candidates and supporters used AI tools to build political bot networks, translate materials, design eye-catching memes, and assist in voter outreach.[7] And election officials experimented with AI to draft social media content and provide voters with important information like polling locations and hours of operation.[8] Of course, AI likely was also used during this election in ways that have not yet come into focus and may only be revealed months or even years from now.

Were the fears and promises overhyped? Yes and no. It would be a stretch to claim that AI transformed U.S. elections last year to either effect, and the worst-case scenarios did not come to pass.[9] But AI did play a role that few could have imagined a mere two years ago, and a review of that role offers some important clues as to how, as the technology becomes even more sophisticated and widely adopted, AI could alter U.S. elections — and American democracy more broadly — in the coming years.

AI promises to transform how government interacts with and represents its citizens, and how government understands and interprets the will of its people.[10] Revelations that emerge about AI's applications in 2024 can offer lessons about the guardrails and incentives that must be put in place now — lest even more advanced iterations of the technology be allowed to wreak irreversible havoc on U.S. elections and democratic governance as a whole. This report lays out the Brennan Center's vision for how policymakers can ensure that AI's inevitable changes strengthen rather than weaken the open, responsive, accountable, and representative democracy that all Americans deserve.

Now is the time for policymakers at all levels to think deliberately and expansively about how to minimize AI's dangers and increase its pro-democracy potential. That means more than just passing new laws and regulations that relate directly to election operations. It also includes holding AI developers and tech companies accountable for their products' capacities to influence how people perceive facts and investing in the resources (including workforces and tools) and audit regimes that will make it more difficult for antagonists to use AI to mislead and disenfranchise voters. Policymakers should also establish guardrails for election officials and other public servants that allow them to use AI in ways that improve efficiency, responsiveness, and accountability while not inadvertently falling prey to the technology's pitfalls.

Whether and to what extent Congress and Donald Trump's administration will prioritize regulating AI remains to be seen. This report provides the following recommendations for both federal and state policymakers, but it is clear that states have a major role to play in 2025 and beyond in strengthening America's democracy in the AI age.

Government Capacity

Governments at all levels — local, state, and federal — must strengthen their capacity to confront the impacts of AI. State and local governments should establish advisory councils to obtain a baseline understanding of AI risks and opportunities to better serve the public. Multiple states have created such entities to help state and local governments to determine whether and how to integrate AI into their operations, though many more have not yet taken such steps.

Federal, state, and local lawmakers should also train staff to use AI appropriately and secure sufficient funding to support safe and responsible AI use. Adequate resources are required to hire and retain top technical and nontechnical AI talent — including computer scientists, cybersecurity professionals, AI risk management experts, and privacy and legal officers — that might otherwise be drawn to more lucrative opportunities in the private sector. These

personnel are essential to ensuring that government departments, offices, and agencies can deploy AI with appropriate safeguards.

Transparency Requirements

Congress and state legislatures should require greater transparency for AI-created and curated election content. Lawmakers should require AI developers, social media platforms, and search engines to publish information on AI-generated election content and AI-assisted design features. Requirements should include information concerning the volume of political deepfakes present on or produced by platforms and tools, implementation of watermarks and content provenance standards, and policies pertaining to responsible dissemination of AI-generated election content.

Congress and the states should also require transparency around generative AI tools' training data. To counter the risk that AI-generated content will be used, among other things, to mislead voters with highly personalized and false information about elections, lawmakers should require generative AI developers to publicly disclose the sources of their original training data sets and of any training data sets under their control used to customize AI systems for particular uses.

Data Safeguards and Corporate Accountability

Congress and state legislatures should ensure that AI developers and system providers can be held liable for harms that their products cause. Congress should explore clarifying that Section 230 liability immunities — which generally shield online platforms from being held liable for content posted by their users under the 1996 Communications Decency Act — do not apply to generative AI developers and deployers.[11] Federal and state lawmakers should also pass laws that make it easier to sue AI developers by requiring them to exercise reasonable care to prevent certain foreseeable harms to voters and the election process.

Additionally, Congress and the states should pass new data privacy protections. Legislatures should regulate generative AI models' collection, use, and processing of personal data to (among other potential concerns) mitigate malefactors' ability to use AI tools to manipulate or intimidate voters or election officials with such data. Such protections could include, at a minimum, limiting personal data collection to use for authorized purposes and giving users the power to opt in to collection of personal data through their interactions with AI models and to companies' ability to sell or release data to third parties — granting users greater autonomy over their personal data and empowering them to make informed decisions about how their information is collected and used.

Civic Participation Protections

Congress and the states should authorize government agencies to disregard misattributed comments on proposed regulations. The federal Administrative Procedure Act and state analogues typically require agencies to solicit, consider, and respond to public comments on proposed regulations.[12] Lawmakers should update these statutes to allow agencies to disregard comments that falsely impersonate others, are transmitted via bots, or are otherwise incorrectly attributed — all of which will become easier with the assistance of generative AI — and to safeguard consideration of authentic submissions.

Federal and state governing bodies should also expand opportunities for real constituents to offer policy input, including by providing ample avenues for public comment that are less vulnerable to technological manipulation, such as surveys built into the process of public benefits administration and those that rely on address-based recruitment, as well as in-person events and town halls.

In addition, federal lawmakers and state agencies should establish guardrails for responsibly using AI to solicit and respond to constituent feedback and questions. Although AI holds significant potential to enhance government's responsiveness capacity, its use does engender risks. Federal lawmakers should clarify that the use of AI to analyze comments on proposed federal regulations — and for other highly consequential processes like soliciting input on essential government services — is a use that directly affects people's civil rights, warranting compulsory protections, including minimum thresholds for accuracy, safeguards against harmful bias, and transparency guarantees. State agencies should impose similar requirements.

Political Communications Regulations

Congress and the states should require disclosure of deepfakes and other manipulated media in political communications. These requirements should apply to candidates, parties, and other political groups that create and disseminate visual and audio content in ads or like communications. They should cover content that is arti-

ficially generated or created or substantially modified with the assistance of digitization, such that the content would leave a reasonable viewer or listener with a significantly different understanding of the speech or events depicted than those that actually occurred. Laws should also mandate clear, easy-to-understand disclaimers informing viewers and listeners that such content has been manipulated.

Major online platforms should also be required to include such information in any public files on political ads sales that they maintain and to use state-of-the-art tools to detect and label a subset of other political content generated or substantially modified by synthetic means. Alongside mandating these disclosures, Congress and state legislatures should consider targeted prohibitions for especially harmful and deceptive election-related content.

Moreover, Congress and state legislatures should require labeling for a subset of content produced by large language models, or LLMs (such as ChatGPT and its latest successor, GPT-4, along with Google's PaLM and Meta's Llama), including when LLMs power interactive chatbots and social media bots deployed by candidates, parties, or other political groups. Such chatbots and social media bots should carry labels informing viewers or listeners of their artificial nature.[13]

Voter Suppression Prohibitions

Congress and the states should strengthen deceptive practices laws and bills to more thoroughly cover deceitful and intimidating AI-generated content. Lawmakers should amend laws and bills that curb the knowing and intentional dissemination of falsehoods about where, when, and how to vote so that they expressly cover AI systems and better limit risks from AI developers who might deliberately design AI tools to disenfranchise voters.

Federal and state legislators should also pass laws prohibiting the knowing and intentional dissemination of deepfakes with strong potential to suppress votes within 60 days before elections. Examples include synthetic content falsely depicting inaccessible polling places, impediments to the use of voting equipment, or election officials preventing or hindering voting.

Additionally, Congress and the Federal Communications Commission (FCC) should bolster the regulation of political robocalls that use generative AI. For one, Congress should close the loophole in robocall regulations that allows political robocalls to be made to landlines under certain conditions without prior consent.[14] The FCC should also complete the process it began in August 2024 to augment prior express consent rules around generative AI–powered robocalls and clarify that the strengthened requirements would apply to political robocalls made to mobile devices.

Election Security Defenses

Congress and the states should boost funding to increase defenses against cyber threats amplified by AI systems. As new AI developments elevate the risk of cyberattacks on election infrastructure, election officials need additional resources and support to implement safeguards, mitigation measures, and security best practices, including the creation of statewide cyber navigator programs to assist local jurisdictions with cybersecurity needs, replacement of outdated equipment, investment in resiliency, and training and education around AI-enhanced security threats.

Relevant federal and state agencies should invest in tools that will allow election offices to embed digital authentication markers in official content. State and federal agencies, starting with the Cybersecurity and Infrastructure Security Agency (CISA) at the federal level, should work with election offices to test and use these tools moving forward. Private-sector partners could be invaluable in developing and deploying such tools.

Congress and the states should fund election offices to educate voters about AI. State and local election officials, along with other government offices, will need to launch voter education campaigns to prepare the public for AI-related changes and challenges in the coming years.

Furthermore, Congress should require independent federal oversight of election vendor security practices. Just as election offices are likely to be targets of AI-enhanced security threats, election system vendors are also logical targets. The federal government should mandate election security best practices for vendors in the elections space — including robust system and network protections and resilience planning — as it does for vendors in other sectors whose assets, systems, and networks have been designated as critical infrastructure.

Election Administration Standards

Relevant federal and state agencies should develop guidance and baseline standards for election officials on how and when to use AI, and they should oversee the creation of an incident reporting system so election officials and others can report AI-related harms. These steps would enable election officials who choose to integrate AI into their work to do so as safely and responsibly as possible. Congress and state legislatures should allocate funds for state and local election offices to implement those guide-

lines and standards, as well as for the monitoring, auditing, and red-teaming (which involves controlled attempts to breach an organization's system to uncover security vulnerabilities) that will be necessary going forward.

Federal and state lawmakers should also require audits, especially for vulnerable and high-risk election systems that utilize AI. Such systems include those used to identify potentially ineligible voters or others who might be removed from voter rolls; those used to verify voters' identities; and those used to provide election information to voters on how to vote, where polling places are located and hours of operation, and what forms of ID might be required.

Finally, Congress and the states should regulate the most sensitive rights-affecting AI use cases in election administration. In many jurisdictions, election officials use AI-powered tools to assist in maintaining voter registration databases and to verify mail ballot signatures, both rights-affecting use cases that necessitate specific additional safeguards such as algorithmic bias testing and error rate monitoring to catch inaccuracies and help mitigate biases. These guardrails must include human involvement in reviewing AI-assisted decisions — particularly for cases flagged as high-risk — as well as regular audits and evaluations of AI systems to ensure effectiveness and compliance with baseline standards.

■ ■ ■

Several campaigns, foreign adversaries, and even some election officials experimented in significant ways with AI in 2024, but it does not currently appear that AI itself radically transformed their operations. In retrospect, that may not be particularly surprising, given how new the technology is. But the piloting seen in 2024 will almost certainly become more integrated into both attacks against and defenses of our elections and democracy in the next few years: Despite the enormous investment in AI globally since 2022, widespread adoption of AI tools across U.S. companies is not projected until the second half of the decade.[15] The same is surely true of AI's use in elections and democratic processes.

I. Government Capacity

Artificial intelligence is a revolutionary technology projected to transform society as much as the development of railroads, cars, and the internet. As with other powerful new technologies, governments at the city, county, state, and federal levels must consider how AI will affect their respective abilities to deliver services while ensuring that any new initiatives do not inadvertently impede citizens' rights and opportunities — or governance obligations to their constituencies writ large.

Progress on this front has been mixed. Several states have made headway by setting up advisory councils, task forces, or working groups.[16] But much more needs to be done, especially at the county and local levels. State, local, and tribal governments that have not yet done so should promptly assemble such advisory bodies to inventory existing AI use cases and identify risks and opportunities associated with AI use. Then, after obtaining a baseline understanding of the technology's potential benefits and risks, they should establish governance structures to create policies and manage implementation and use. These governance bodies should initially focus on developing policies around transparency, public feedback, civil rights and liberties, anti-bias, and privacy protections to safeguard citizens' rights and opportunities.

In October 2023, the Biden administration moved to outline and institutionalize governance oversight structures for responsible AI deployment. Executive Order 14110 introduced federal government–wide coordination processes and initiated the creation of policies to manage agencies' use of AI.[17] On January 20, 2025, President Trump repealed that order as one of his first actions in office.[18] How the Trump administration may address AI in the future is not yet clear — a reality that underscores the important role that states will likely play over the next four years.

Governing bodies have a long list of issues to address, but they should start by protecting vital freedoms. Americans need federal and state lawmakers to build comprehensive governance frameworks that ensure responsible government use of AI and to establish bulwarks against its risks. The steps outlined below represent preliminary actions that executive agencies and legislatures should take to construct those crucial safeguards. Where state, local, and tribal governments determine that they lack the resources necessary to take these steps on their own, they should consider entering into compacts with neighboring jurisdictions to pool resources. The following recommendations offer a road map for federal, state, and local governments and legislative bodies to follow with regard to capacity-building.

>> Develop a baseline understanding of AI's risks and benefits.

State and local governments need to build a solid understanding of AI's potential risks and how to address them, as well as how to harness its beneficial uses safely and responsibly. States including Georgia, Massachusetts, Oregon, and Tennessee have taken steps in this direction by launching advisory councils and task forces.[19] The Louisiana and Pennsylvania legislatures have also formed state-level bodies to advise state governments.[20] At the federal level, in addition to the now-repealed 2023 executive order, the National Artificial Intelligence Initiative Act of 2020 created the National AI Advisory Committee to convene experts from across the private, nonprofit, and civil society sectors and academia to advise the president on topics related to AI.[21] Pursuant to the 2023 executive order, several federal government agencies also designated chief AI officers, though it is unclear as of this writing what role those officers will have, if any, under the new administration.[22]

Some other states offer models to look to as well: In 2023, Minnesota's executive branch IT services agency convened a group called the Transparent Artificial Intelligence Governance Alliance to examine AI policy, governance, and use issues and to develop processes and structures for safe AI deployment.[23] And in 2024, Utah's Department of Commerce launched the Office of Artificial Intelligence Policy (OAIP), which enlists academics, industry leaders, and other experts to advise the state legislature on effective methods of AI regulation.[24]

States that follow suit in creating such AI advisory bodies should recruit technical experts — including academics and private-sector specialists — along with privacy, civil rights, and civil liberties professionals, lawyers, and representatives from departments and agencies planning to adopt AI. These bodies should be permanent to reflect the continuing evolution of AI and its ongoing effects.

Congress and state legislatures should also build their AI knowledge base. High-priority topics include ensuring

safety when using AI to improve legislative branch services for citizens, promoting effective oversight, developing appropriate regulations, and appropriately funding executive branch AI work.

At the federal level, one way to build this knowledge is by expanding the Science, Technology Assessment, and Analytics office within the Government Accountability Office (GAO). This office should create a new science and technology hub to compile and disseminate science research to committees and members and to connect Congress with technical experts.[25] It could then convene expert advisory panels — similar to the executive branch advisory committees and those at the National Academies of Sciences, Engineering, and Medicine — to construct an institutional knowledge base on AI.[26] This hub could also translate technical information for legislative committees as they navigate complex issues around AI's emerging fields.

Additionally, local and state legislative entities should consider establishing temporary committees to jumpstart their understanding of AI issues and leveraging executive branch entities for this support.

>> Establish effective structures for oversight and regulation in federal, state, and county legislatures.

Lawmaking bodies should reorganize their committee structures to effectively regulate AI. A basic step for Congress to take is to create a dedicated technology committee.[27] The last reorganization of legislative committee jurisdictions in Congress occurred in the 1970s, before the development of the internet.[28] As a result, multiple committees have held overlapping hearings on AI: Since 2023, committees including the Senate Judiciary Committee, the House Committee on Oversight and Accountability, the Senate Committee on Rules and Administration, and more have held hearings on topics ranging from *Oversight of AI: Rules for Artificial Intelligence* and *Oversight of AI: Principles for Regulation* to *AI and the Future of Our Elections* to *Addressing Real Harm Done by Deepfakes*.[29]

Too many proverbial cooks in the kitchen inevitably make it more likely that details will fall through the cracks: One committee could neglect to share details with another, different committees could overlap in their work, and committees may focus on piecemeal legislation that ought to be treated more holistically. A dedicated committee would allow Congress to regulate the technology sector — including AI — more efficiently and comprehensively. State legislatures should also consider establishing primary committees charged expressly with addressing the AI-related issues raised in this report (and many more certain to arise).

>> Create mechanisms for state and local governments to manage the implementation of AI.

After obtaining a baseline understanding of AI's possible pitfalls and promises, local and state governments will need to develop governance mechanisms to manage the incorporation and continued use of the technology by establishing internal department and agency authority and rules for AI deployment.

Departments and agencies leveraging AI should create boards of stakeholders from across their organizations to assess AI use before, during, and after implementation. For example, under the recently revoked 2023 executive order on AI, the federal government required departments and agencies to appoint chief AI officers and to establish internal AI governance boards chaired by deputy secretary–level officials.[30] According to the Office of Management and Budget (OMB), these boards were to include "appropriate representation from senior agency officials responsible for . . . AI adoption and risk management, including at least IT, cybersecurity, data, privacy, civil rights and civil liberties, equity, statistics, human capital, procurement, budget, legal, agency management, program evaluation, and officials responsible for implementing AI within an agency's program office(s)."[31]

Such governance bodies should clearly define decision-making authority, including the ability to enforce AI policies and develop guidelines. They should also require senior leaders to oversee AI governance: The potential ramifications of AI misuse are too great for governance mechanisms to reside deep in bureaucracies. These boards should be prioritized and managed by senior leaders in government.

To fully realize these goals, legislative bodies must adequately fund departments' and agencies' initiatives aimed at safely and appropriately adopting and deploying AI systems.[32] Without sufficient funding, governments at any level will find it difficult to responsibly and effectively adopt and deploy AI while safeguarding security, accuracy, reliability, and fundamental rights.

>> Build transparency, public feedback, and human oversight policies and procedures.

Constituents should be aware of and able to comment on how the government uses AI, which can best be achieved by creating online portals or forums for providing feedback. For instance, Utah's OAIP held an open AI summit in October 2024 to discuss and strategize on Utah's advancements in AI, policy development, regulatory relief, responsible AI implementation, and workforce readiness.[33] In November, the OAIP issued a public call for input from technology leaders and other community members on issues including liability and legal protections for AI development and

deployment; AI in health care and education; privacy and AI; and deepfakes and their implications.[34]

At the federal level, in November 2023 (two days after President Biden's executive order), OMB released for public comment a new draft policy on advancing governance, innovation, and risk management for government-wide use of AI technology. The guidance established AI governance structures in federal agencies, advanced responsible AI innovation, increased transparency, and implemented risk-management procedures for government uses of AI.[35] Furthering the effort to "establish transparency mechanisms to drive and track implementation of these practices," and "to help ensure public trust in the applications of AI," OMB and the White House launched a website where the public could comment on the draft guidance, which was finalized in March 2024.[36] (President Trump has directed OMB to revisit this policy.)[37]

These new governance structures are promising examples of safety, accountability, and responsiveness measures that local and state governments should adopt as well. And they should be paired with public notification and human review of AI-assisted actions and decisions that could directly affect civil rights and liberties, privacy, and public safety, so that constituents can request appeals if they experience harm from AI systems. Governments should also implement demonstrably effective internal and external quality control processes and conduct regular performance audits of AI systems, publishing accessible reports on their accuracy, reliability, and any adverse outcomes.

>> Develop and implement civil rights and liberties, anti-bias, and privacy protections.

Governing bodies should establish guardrails to protect civil rights, civil liberties, and privacy. According to a March 2024 OMB memo, the federal government presumes that AI use in elections is "safety-impacting" or "rights-impacting" if it is used to "control or meaningfully influence" agencies' work to maintain the "integrity of elections and voting infrastructure."[38]

All government departments and agencies should review each AI system they use to determine whether it impacts rights and designate circumstances in which use of AI systems would be presumed to do so. If a particular AI tool or use is found to impact rights or safety, then officials must seek to eliminate or sufficiently mitigate harmful outcomes or discontinue use of the tool.

As part of this process, agencies should conduct impact assessments with documentation to evaluate both risks and positive outcomes to confirm the benefit of a particular AI system's continued use.[39] If agencies opt to continue using the tool or system, then they should follow adequate risk-mitigation and security practices, continue monitoring the tool's risks and impacts, properly train staff operators of the tool, and notify the public of its use.

>> Incorporate risk management procedures.

State and local governments should develop or adopt standards to assess and mitigate risk before, during, and after the deployment of AI systems. The federal government has already made progress in this regard: The National Institute of Standards and Technology (NIST) published its *Artificial Intelligence Risk Management Framework* in January 2023 for voluntary use by AI deployers and developers.[40] In July 2024, NIST published a companion guide, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, for government-wide "trustworthy and responsible" generative AI use as directed by the Biden administration's 2023 executive order on AI governance.[41] And in November 2024, the Department of Homeland Security (DHS) too published guidelines for governance of AI use in critical infrastructure sectors.[42]

These products can help organizations identify AI-related risks and ways to manage them. Nonetheless, considerable additional work and expertise is needed to identify context-specific risks and mitigations and to assess individual AI systems that might be sought out for particular purposes. Relatedly, government agencies should implement procedures to make sure that when they employ AI or other automated processes to make or assist in making decisions about individual rights — such as determining eligibility for benefits or directing enforcement actions — they provide the affected individuals with the information needed to understand AI's role in the action or decision as well as the opportunity to challenge it.[43]

>> Prioritize recruiting and retaining AI talent.

To ensure safe and appropriate AI use, governments should prioritize hiring and retaining experts. While the need for individuals with technical AI knowledge is a given, recruiting experts in privacy, civil rights and civil liberties, policy development and implementation, and cybersecurity will add a layer of protection for citizens whose rights might be infringed upon.

The market for such talent is highly competitive, but the public sector holds potential professional advantages, like the ability to partner with state colleges to develop internship and fellowship programs in relevant disciplines such as engineering, computer science, AI, law, policy, and cybersecurity. State and local governments can also make exceptions to their strict hiring policies, provide more competitive compensation, and institute generous student loan repayment programs for individuals with AI expertise.

Pennsylvania offers one model to follow. The state is planning to create a two-year fellowship program for post–bachelor's, master's, and doctoral candidates to work with state agencies on AI issues.[44]

>> Train current government employees on AI use and corresponding threats.

The current workforce at all levels of government will need training on the AI systems their organizations choose to adopt and on how to use them safely and appropriately, and on the ways that AI use increases cyber threats, particularly phishing attacks. Governments should also incentivize existing employees to bolster their AI skills, perhaps with stipends or by offering to pay full tuition for advanced courses on AI-related technical, legal, policy, cybersecurity, privacy, civil rights, and civil liberties issues.

The federal government should build on the steps it has already taken to ensure responsible AI use. Even as the prospects for additional reforms are unclear in the new administration and Congress, threats persist, including an ever-increasing cybersecurity threat environment for federal IT infrastructure. AI systems and their operators will almost certainly become more proficient at phishing attacks, putting sensitive data — including U.S. citizens' personal data — at greater risk of exposure.[45] The federal government must prepare the workforce for this heightened threat environment. To that end, CISA, in coordination with NIST and other applicable departments and agencies, should develop and deploy training programs for the federal workforce on AI-enabled cyber threats.

>> Explore how AI can make government more efficient and responsive without adverse impacts.

AI has the potential to improve public services, including by increasing efficiency and providing government departments and agencies with tools to help brainstorm new ideas. Governments should identify ways to do so while also establishing and implementing robust risk management practices — including requirements to halt the use of AI tools whose risks cannot be adequately mitigated.

Countless companies peddle AI software solutions to help government agencies improve government efficiency and responsiveness. But, as the Brennan Center has noted, AI (and generative AI especially) can diminish government's responsiveness as well — for example, by undermining the public comment period, the primary mechanism for incorporating public input into the federal regulatory process.[46] More specific to elections, the Brennan Center has extensively explored the opportunities that AI integration presents for increasing election administration efficiency and improving the voter experience, but also the risks that it poses, which the next section delves into.[47]

II. Transparency Requirements

How does AI-generated and curated content influence U.S. society and democracy? There are some things we know: algorithms control what users see; content moderation policies are not applied consistently and may not be detailed publicly; and misinformation can spread quickly, unchecked. But how algorithms influence what users see is much harder to determine, and ascertaining the overall effects on democracy is all but impossible without behind-the-scenes information on how companies operate tools and run platforms.

Even the strongest existing laws requiring transparency for AI-curated and generated content online are limited. The European Union's 2022 Digital Services Act (DSA) targets services such as social media platforms operating in the European Union and offers limited oversight of generative AI systems. The European Union's 2024 Artificial Intelligence Act largely applies only to products placed on the market or put into service in the European Union.[48] The EU AI Act imposes transparency obligations on so-called "general-purpose" generative AI systems, such as disclosures on system functionality and training.[49] But it leaves a regulatory gap because it does not require that generative AI companies disclose their efforts to override models' responses to election-related questions or the volume of deceptive content that their tools generate, for instance.

Transparency measures in the United States continue to face legal challenges, but the outlook for well-designed statutes remains promising. Although the Ninth Circuit recently temporarily blocked portions of a California transparency law, the Supreme Court evinced a substantially more favorable view of transparency laws' constitutionality earlier in 2024: In *Moody v. NetChoice LLC* and *NetChoice LLC v. Paxton*, a majority of the Court indicated that it would apply a particularly relaxed form of constitutional scrutiny — the compelled commercial speech standard governing "factual and uncontroversial" information about terms and services — to an expansive array of transparency provisions in the context of social media regulation.[50]

The Ninth Circuit panel attempted to draw a distinction between the California law and the Florida and Texas laws at issue in the *NetChoice* cases. But the Supreme Court stated that it would apply the looser standard to laws requiring platforms to give detailed explanations for content moderation decisions, signaling that it would be lenient toward laws that compel companies to disclose when and why they shape or limit content produced or hosted by their tools.[51] Given this nod from both liberal and conservative Supreme Court justices, legislators should not shy away from enacting prudent AI transparency laws such as those recommended below.

>>Strengthen transparency frameworks for AI-created and curated election content.

Congress and state lawmakers should work to pass more comprehensive transparency measures that apply to generative AI systems, social media platforms, and search engines. These legal frameworks need to better capture generative AI–based election content appearing on social media platforms and in search engine results and shed more light on platforms' use of AI to curate and present election content. Additional transparency would better inform the public and enable regulators to make smarter decisions. The recommendations below are not exhaustive; they are intended to complement requirements in the European Union and the California law mentioned above, and others.

Alongside a broader transparency framework, certain entities should be required to continuously provide certain information directly to the public — including a subset of generative AI developers that build general-purpose generative AI models and systems (as defined by the EU AI Act) used in America.[52] Among other elements, transparency law requirements should include the following:

- **Terms of use related to elections:** General-purpose generative AI developers should be required to publish their terms of use for all publicly available tools in a way that ordinary users can easily understand, including by describing any restrictions on acceptable election-related use.

- **Content moderation policies related to elections:** Large social media companies and search engine providers should be required to publish content moderation policies pertaining to election-related information and election falsehoods, including policies that address generative AI.

- **Blocked or redirected generative AI election queries:** Developers that make general-purpose generative AI tools available to the public should be required to disclose

whether they override the underlying models' outputs to stop chatbots and other generative AI tools from answering certain election questions or producing political deepfakes. If so, then they should be required to publish high-level descriptions of prompts that are blocked or filtered. They should also be required to disclose whether they redirect users to other sources of election information and, if so, what those sources are.

- **Usage rate limits:** General-purpose AI developers should be required to disclose whether they have usage rate limits (i.e., limits on the number of times a user can use services within defined time frames) for their tools' user interfaces (UIs) and application programming interfaces (APIs). Developers should also be required to publish information about the limits' thresholds. Such usage rate limits are important safeguards against bot-driven activity and deceptive influence campaigns.

- **Watermarking and content provenance:** General-purpose generative AI developers should be required to disclose whether (and which of) their content includes maximally indelible watermarks and content provenance information. They should also be required to publish information on where to access and how to use any associated watermark and provenance decoders.

Several large online platforms and generative AI developers already provide some public information on their terms of use, content moderation policies, usage rate limits, and watermarking and content provenance practices — but such information is not always comprehensive and is not consistently required by law to be provided to all U.S. users.

In addition to certain continuously published information, federal and state laws should require large social media companies, general-purpose generative AI developers, and large search engines to publish quarterly transparency reports that include the following information:

- **The volume of manipulated political deepfakes on social media:** Large social media companies should be required to publicly release details on the volume of manipulated media identified and restricted under platform policies or otherwise, disaggregated by election and non-election content categories.

- **Election-related use of generative AI tools:** General-purpose generative AI developers that produce tools with a large U.S. user base should be required to publish information on election-related use. This information should include the volume of identified accounts that contravene election-related terms of use and associated enforcement of relevant usage policies; how many election prompts are blocked or redirected because the prompts risk incorrect or problematic results; the number of accounts associated with those queries; and the number of blocked attempts to produce election-related misinformation at scale through APIs.

- **Algorithmic choices that affect elections:** Large social media companies and search engines should be required to explain algorithms that are designed specifically to target election-related information and misinformation, including factors that affect how content is ranked and recommended to users. Large search engine providers should also be required to identify any categories of election-related searches that will produce an AI-generated overview in search results to the extent that such identification is technically feasible.

- **Election integrity staff and resources:** Large social media companies, search engine providers, and generative AI companies should be required to provide information on the volume of election integrity staff working at the company. Those figures should include the numbers of U.S.-based staff members fluent in the most commonly spoken languages in the United States, including Spanish, dialects of Chinese, Hindi, Tagalog, and Vietnamese.

- **Disaggregated information:** Large social media companies, search engines, and generative AI developers should be required to provide the above information disaggregated by major language category and country.

>> Legislate additional monitoring and assessment of AI risks via attack surfaces.

Secured AI systems like ChatGPT, Google's Gemini (formerly Bard), and Anthropic's Claude limit access to the model weights, or numerical values, that underpin the model's production of content. Companies that make these tools often also have usage policies that prevent the tools' use in political campaigns and can block users from creating realistic deepfakes of politicians or other public figures. But unsecured open-source or open-weight AI systems differ in that their model weights are public, making it easy for users to modify or remove any built-in safety features.[53]

Because anyone with malicious intentions can modify unsecured AI systems on their own hardware, determining the extent of uses harmful to elections and civic institutions is impossible. That said, researchers have techniques to better understand some of these uses. Many such techniques require access to data about a system's attack surfaces — the points in a system or software environment that malefactors might use to try to attack elections or manipulate democratic discourse, like social media platforms and search engines.

Federal and state lawmakers should look to the European Union's DSA as a model for addressing these concerns with measures that go beyond the transparency recommendations outlined above. The law places requirements on very large online platforms (VLOPs) and very large online search engines (VLOSEs).[54] If adapted to comport with U.S. law and adopted in the United States, such requirements would greatly assist in identifying the scale of unsecured AI systems' harmful uses without necessarily falling afoul of the First Amendment or infringing on privacy. Examples include requiring VLOPs and VLOSES to

- assess the risks that their products pose to elections and democracy and then share those risk assessments with regulators and eventually the public;[55]
- put plans in place to minimize the assessed risks and execute on them transparently;[56]
- ensure that the risk assessments and mitigation plans are independently audited and reported on;[57] and
- allow vetted researchers access to real-time and historic platform data to evaluate all of the above.[58]

Similar requirements in the United States, tailored to First Amendment principles, would enable researchers to look for patterns of harmful use traceable to unsecured AI systems. Such patterns could indicate coordinated, AI-aided, inauthentic behavior along with information leveraged in attempts to breach election systems' security defenses.

>> Require transparency regarding generative AI tools' training data.

The risk of highly personalized AI-generated content designed to manipulate voters, candidates, or election officials spreading before an election is a critical vulnerability. This content could be disseminated through customized emails, interactive chatbot conversations, voicemails, phone calls, or even video calls. Such tools would likely be fine-tuned on custom data sets of election disinformation and personal data based on well-honed manipulation techniques.

As a safeguard against these and other risks, federal and state lawmakers should require generative AI developers to publicly disclose the sources of their original training data sets and of any training data sets under their control that are used to customize AI models and systems for specific uses (such as chatbots that answer questions about voting). They should also require developers to publish the types and volume of data in their training data sets, share information on the ownership of the data sets and how they were obtained, and disclose whether the training data includes personal information. The latter would be especially pertinent when training data includes personally identifiable information such as voter roll data or other sensitive information about individuals purchased by data brokers or obtained through illicit or questionable means.

III. Data Safeguards and Corporate Accountability

Current liability rules fall short when it comes to AI developers, who are at least partly responsible when their tools prevent people from voting or generate political deepfakes. But lawsuits seeking to establish their negligence face a high bar: When AI systems contribute to election-related harms, negligence can be difficult to show in many situations because the injury might not be recognized under the negligence standard, or because the scope of AI developers' legal duty to exercise care to protect the large numbers of people affected by AI-assisted decisions and exposed to AI-generated content is not clear.

Other legal frameworks don't fare much better. Virtually all deepfake laws target the deepfake's distributor or creator (i.e., the user of the tool that creates the deepfake) rather than the tool itself.[59] Defamation law protects criticism of public figures by requiring would-be defamers to demonstrate "actual malice" — knowledge or reckless disregard regarding the falsity of their claim — a standard that makes it difficult to hold companies responsible for content produced by AI tools that lack sentience.[60] Laws like the Voting Rights Act, meanwhile, allow voters to sue state and local governments to remedy discrimination, but they typically do not provide robust avenues for bringing civil suits against companies. And although Section 230 of the Communications Decency Act — a liability shield for online platforms — *might* not protect generative AI developers from lawsuits, courts have yet to conclusively rebuff the act's applicability to generative AI. The recommendations below suggest ways to improve the legal frameworks for holding AI developers accountable and protecting people's personal information.

>> Pass laws to hold AI developers responsible for harming voters and the election process.

Congress and state legislatures should pass laws that make it easier to sue AI developers for harming voters and the election process.[61] These laws should specify that AI developers have a duty to take care to prevent reasonably foreseeable election-related harms. Laws should allow affected individuals and attorneys general to seek injunctive relief and civil penalties when AI tools are the cause of, for example, reasonably foreseeable voter disenfranchisement in election administration; dissemination of content that substantially risks disenfranchising voters; or dissemination of unwatermarked AI-generated political deepfakes that deceptively depict candidates or election officials in a material manner during the period before an election. These laws should not replace separate liabilities for those who deploy AI to administer elections or reach large numbers of voters, such as election offices and campaigns.

>> Consider clarifying Section 230 liability for generative AI developers.

Section 230 of the Communications Decency Act generally shields social media companies and certain other digital entities from liability in lawsuits that arise from content created by third-party users.[62] Federal lawmakers should consider whether they should pass a law making clear that Section 230 does not give generative AI companies immunity from lawsuits arising from their models' outputs, including election falsehoods and deepfakes.[63] Courts have not yet fully clarified Section 230's applicability to generative AI models.

A strong argument can be made that generative AI systems do not squarely meet the requirements for Section 230 immunity. The law shields companies from a large number of lawsuits if they qualify as "interactive computer service" providers (which generative AI companies typically are) and they display content "provided by another information content provider."[64] Several courts have found that the shield does not apply when a company "materially contributed" to the content's alleged illegality.[65]

Whether generative AI tools meet the second criterion of producing content "provided by another information content provider" is debated, but a compelling case can be made that they do not. Although generative AI tools vacuum up large swaths of content created and published online, their outputs often do not perfectly replicate that third-party content.[66] Rather, the precise combination of words produced is the result of complex algorithms that are underpinned by statistical probabilities and, often, extensive developer-led training processes and human feedback loops that nudge models toward certain answers and away from others.[67]

There is good reason to leave this issue out of the courts, which are not well-equipped to make policy by interpreting statutes that were not designed for the advent of AI. Congress should instead explore passing a law clarifying that Section 230 immunity does not apply to generative AI providers. One effort to that effect worth serious consideration — which was referred to the Senate Committee on

Commerce, Science, and Transportation during the 118th Congress — was S. 1193, which would have denied Section 230 immunity "if the conduct underlying the claim or charge involves the use or provision of generative artificial intelligence by [an] interactive computer service."[68]

>> Limit election offices' processing of personal data and transmission to outside brokers.

Nearly every stage of the election cycle involves collecting and processing voters' personal data, from registering and authenticating voters, which sometimes involve AI-enhanced methods, all the way to transmitting election results. AI systems pose serious privacy-related risks because of how they collect and manage personally identifiable information.[69]

As election offices increasingly integrate AI into their work, such technologies risk eroding voters' privacy. Malefactors with access to voters' data — like detailed demographic information, financial and medical information, and nuanced information about political preferences — could deploy AI tools to manipulate voters' vulnerabilities, concerns, and fears. Well-funded and organized groups could exploit personal data sold or released by AI developers to intimidate election officials and voters.[70] And along with the hazards mentioned above, personal and other sensitive data is also vulnerable to unauthorized release through cyberattacks and exploitation by corporations amid rising data breaches at election offices.[71]

Congress and state legislatures should set and enforce standards that improve safety when election offices and vendors collect, process, and transmit voters' personal data. Some important protections that limit election offices' ability to sell voter files and disclose certain other types of sensitive election data already exist.[72] However, these restrictions do not cover all the risks that uses of personal data in election office functions entail, including in routine uses, such as when offices transmit voters' information to print vendors and mailhouses or use it to verify requests from constituents made through public-facing websites like online voter registration tools. The security of these uses must be strengthened to better protect voters.

>> Regulate generative AI models' collection, use, and processing of personal data.

The public should have the right to know and control how their personal information is collected and processed by generative AI systems. In addition to the transparency recommendations in the previous section, Congress should pass legislation requiring generative AI providers to give consumers more power over how AI systems collect, use, and process their personal data.

Potential measures include notifying generative AI users about real-time data collection while they are using a model. The California Privacy Rights Act currently uses an opt-in consent standard for consumers under the age of 16, which should be the national standard for people of all ages.[73] The public ultimately needs broader, more comprehensive privacy protections to guard against the full range of privacy risks that generative AI and other technologies engender, including protections limiting companies' personal data collection to uses for authorized purposes only. But the standards discussed here would be a laudable first step.

IV. Civic Participation Protections

Much ink has been spilled over the problem of AI-generated political deepfakes and their potential to manipulate public perceptions of officials. Far less attention has been devoted to the ways in which malefactors can now leverage generative AI to distort policymakers' perceptions of public opinion, particularly through fake AI-generated constituent comments on proposed policies.[74]

A troubling episode from 2017 exemplifies the risk: An army of bots peppered the FCC with more than 1 million artificially generated comments in an attempt to influence the agency's rule-making on U.S. net neutrality policy.[75] The scheme's architects aimed to disguise the comments as those of real, concerned citizens. Investigators uncovered the plot in part because the fake comments were uncannily similar — many used terms, sentence structures, and paragraph compositions that perfectly mirrored one another or were close analogues.

This type of campaign could be replicated to distort executive branch regulatory processes, legislators' perceptions of constituent sentiment, or local governments' understanding of residents' needs. Generative AI could make the practice more pervasive simply by virtue of the scale it could achieve — and more insidious by producing comments that are fluid, persuasive, differentiated, and harder to detect. Research shows that state policymakers cannot distinguish AI-generated outreach from genuine constituent communications without technological aids.[76] And AI detection tools have had limited success in identifying content produced by LLMs, the technology underlying generative AI chatbots.

Unscrupulous stakeholders from regulated industries, chaos agents, or even foreign state adversaries might deploy such AI-powered campaigns to promote their own policy aims and disrupt American democracy. The Federal Trade Commission (FTC) has taken steps to grapple with analogous problems with faked consumer reviews in the business context, but the risks when it comes to public comments on rule-making — and other government decisions and policies — extend to the very ideals of responsive and participatory government in a democracy.[77]

More broadly, federal agencies can receive hundreds of thousands of public comments on high-profile rule-makings. The Administrative Procedure Act requires federal agencies to adequately consider all comments on proposed rules, but the sheer volume of submissions has led to a tendency for regulators to discount mammoth numbers of comments from ordinary Americans in favor of a smaller pool of technical comments from well-educated — and often wealthy — stakeholders.[78]

Legislators and local officials are likewise often overwhelmed with constituent outreach, which imposes substantial opportunity costs and can compromise government responsiveness, keeping residents from accessing vital services. The Congressional Management Foundation estimates that many congressional offices devote about half their resources to fielding constituent communications.[79] Local agencies that administer essential services such as public housing often fail to answer questions from needful residents.[80] And officials' failure to adequately respond to outreach can undermine constituents' trust in government.

At the same time, public input on policies and services itself might not be representative despite this overwhelming volume of public comments. Feedback mechanisms might overrepresent opinions from the most vocal constituents while underrepresenting the viewpoints of hard-to-reach or time-burdened groups such as low-income or immigrant populations.

AI can facilitate public input on governance and improve government's responsiveness to its constituents. But as with any adoption of AI systems in a sensitive context, such use presents risks. AI systems might generate inaccurate analyses or perpetuate biases against groups that speak languages other than English, immigrant groups, people of color, low-income individuals, women, and persons with disabilities — making guardrails imperative. All of these challenges demand a response, which the recommendations below seek to address.

>> Empower governments to disregard fraudulent or misattributed policy input.

Federal and state laws should include provisions that allow agencies to decline to consider comments when compelling evidence indicates that they have been fraudulently transmitted by bots or otherwise submitted using false identities. The federal Administrative Procedure Act and its state analogues typically require executive agencies to consider and respond to public comments on proposed regulations with no express exceptions for those potentially submitted under false pretenses or those that may duplicitously misrepresent how many constituents' views they reflect.[81]

Standards permitting agencies to decline to consider comments when abundant evidence points to fraudulent

origin would not capture constituents who use generative AI to help them write comments, nor would it dismiss anonymous submissions or comments from grassroots groups that ask like-minded constituents to click an online link to submit identically worded comment forms. Rather, it would curb comments designed to sizably and dishonestly skew officials' perceptions of the number of constituents who endorse or oppose a specific policy.

Officials should give ample notice and opportunity to appeal any government determination that comments have been fraudulently transmitted. In making such determinations, agencies should only use automated detection tools to identify fraudulent submissions and bot-transmitted content if those tools meet established and rigorous standards for accuracy, lack of bias, and fitness for purpose, and they are deployed in a way that protects privacy. At the federal level, Congress should direct OMB's Office of Information and Regulatory Affairs to coordinate actions if agencies suspect a deceptive AI-powered campaign.

>> Expand opportunities for real constituents to provide comments on policy and governance.

Certain tools for soliciting public input on policymaking and governance are less vulnerable to technological manipulation, including surveys that rely on address-based recruitment, surveys integrated into public benefits administration processes, and in-person events such as town halls and public hearings. While other tools to gauge constituents' preferences remain invaluable and should be continued, officials should consider increasing these less vulnerable forms of appraising sentiment, which offer distinct benefits if implemented with care.

Surveys can provide invaluable feedback on service delivery and a more representative picture of constituents' views. They might even reveal targeted insights into communities that might otherwise remain insufficiently understood. Town halls and public hearings can be helpful for constituents disinclined to write comments or those whose viewpoints are more effectively communicated face-to-face. Whereas public events can sometimes lack participatory representativeness, that deficiency can be mitigated by promoting geographic diversity, language accessibility, disability accommodations, and extensive outreach.

>> Invest in AI tools to enhance government responsiveness — with proper oversight.

If deployed with sufficient oversight and rules, AI could help governments be more responsive to constituents. With adequate safeguards, it can also assist governance bodies in fielding large volumes of public comments and queries. Agencies and legislative staff could deploy carefully vetted and continuously assessed AI systems to help analyze the massive volume of outreach they receive. Moreover, AI tools could potentially produce a more nuanced accounting of patterns, trends, personal stories, and novel ideas. AI capabilities like clustering and organizing similar legislative texts and summarizing, translating, transcribing, and advising on internal procedures could help overwhelmed and understaffed legislative offices and agencies more effectively assist constituents — as long as AI implementation prioritizes mitigating risks such as inaccuracy and bias.

Provided that accuracy is ensured, using rules-based AI chatbots (that is, chatbots not powered by generative AI that respond to prompts based on sets of defined rules) to answer simple queries can also free up officials' time and help people get answers quickly. Several government agencies currently use non-generative AI chatbots to interact with constituents.[82] These chatbots sometimes employ natural language processing — a subfield of AI that enables computers to recognize human language and generate text and speech in response — or they simply generate pre-vetted answers based on keyword identification.

New state and local initiatives show how AI could be used to collect valuable insights from the public on specific issues.[83] For instance, the Georgia AI Innovation Lab at the state's Office of Artificial Intelligence scrapes legislative data to help citizens and lawmakers find bills more easily and better understand the legislative landscape.[84] New York state is partnering with Google Cloud to use AI to give citizens a voice on issues like health care and the Department of Motor Vehicles.[85] In Charleston, South Carolina, the AI chatbot Citibot allows city residents to flag issues like potholes, broken street signs, and missed trash pickups, prompting automated report aggregation so the city can respond.[86]

>> Establish guardrails for government's use of AI to interact with constituents.

Despite these and other opportunities for AI to promote responsive governance, its use engenders considerable risks. To mitigate these risks, policymakers should create and implement rules and safeguards around government use of AI to evaluate public input on proposed federal regulations and respond to constituent questions, as well as other highly consequential processes for soliciting public input on government decision-making and services.

To start, OMB should clarify that such AI use by federal agencies is one with civil rights, civil liberties, and privacy implications that warrants compulsory guardrails. These protections should include mandating transparency around the government's use of AI for such purposes; affirming systems' continuous fitness for purpose (including establishing minimum thresholds for AI system accuracy and continually checking for and

remedying unacceptable bias); and requiring a baseline level of human involvement in evaluating constituent feedback.

State and local governments should adopt similar protections. Where standards do not exist, officials should carefully assess AI systems to mitigate their potential risks. The first step should be determining whether use of an AI system is appropriate for a given context. Officials should also evaluate and prepare for AI systems' performance across different scenarios and data sets; train staff on appropriate use; plan for measures to address possible system failures; and make sure that humans are involved in all AI-assisted functions.

At this time, government bodies should not provide generative AI chatbots to answer constituent questions, as the accuracy of such tools cannot yet be guaranteed. However, governments could deploy public-facing non-generative AI chatbots as long as they are adequately and continuously tested for response accuracy, regularly evaluated for fitness for purpose, and routinely audited for bias, and they do not exacerbate language access issues.

V. Political Communications Regulations

Deepfakes and other deceptive AI-generated content have played an increasingly prominent role in election campaigns both in the United States and abroad. AI-generated images of both major U.S. party nominees for president circulated widely on social media in 2024.[87] And on the eve of the 2024 New Hampshire primary, AI-generated robocalls mimicking President Biden's voice targeted voters to discourage them from participating.[88] Deepfakes are playing a greater role in down-ballot races too, such as a recent ad featuring an AI-generated video of North Carolina GOP gubernatorial candidate Mark Robinson.[89] AI factored even more prominently in other countries' national elections.[90]

Outside of the electoral context, deceptive AI content's role in other political disinformation campaigns has accelerated, including those linked to hostile foreign governments. One widely circulated video, seemingly from Russia, purports to show a U.S. State Department official suggesting that a Russian city is a legitimate target for Ukrainian strikes using American weapons.[91] At the same time, not all AI-generated content is necessarily harmful: Sometimes it can be used for innovative political messaging. For example, in Belarus — which is effectively a dictatorship — the opposition party endorsed a candidate for parliament who was actually a chatbot as a way to underscore the point that the country's parliamentary elections were not free and fair.[92] And in Pakistan, opposition leader Imran Khan used an AI-generated video to address his supporters from prison.[93]

The range of ways that AI-generated content is affecting the political process points to the need for a careful regulatory approach, one that guarantees voters and the broader public access to accurate information about the messages they receive without unduly suppressing political expression. In the United States, such an approach is not merely advisable as a policy matter but constitutionally required: Under prevailing Supreme Court jurisprudence, even vital government interests are often deemed insufficient to justify certain restrictions on political advertising. But the Court has also noted in analogous contexts that the government has a compelling interest in promoting an informed electorate, and that requiring transparency does not "prevent anyone from speaking," which has led courts to uphold many campaign finance transparency rules, for instance.[94]

Deepfakes have been the subject of more regulatory attention than any other area related to AI and elections. Between January 1 and July 31, 2024, state lawmakers introduced or passed 151 bills regulating deepfakes or deceptive media, making up one-quarter of all AI bills across the country.[95] Many states have instituted disclosure requirements for political communications, mandating labels for AI-generated campaign ads. In 2024, California became the first state in the nation to require large online platforms to develop and implement procedures to label and take down materially deceptive political deepfakes.[96] A few states have gone farther and sought to ban some political deepfakes outright (though how extensively such rules are actually enforced is unclear).[97]

Congress has been slower to regulate AI, but lawmakers introduced hundreds of AI bills across a range of issues during the 118th Congress.[98] Federal agencies have also taken some tentative steps related to AI in political communications — primarily clarifying that certain of their existing rules apply to AI-generated deceptive content. It remains to be seen what additional steps will be taken in the new presidential administration.

Other countries too are moving to impose more regulation on political deepfakes. Most notably, the 2024 EU AI Act includes strict transparency requirements for all AI-generated deepfakes as defined by the act, including those related to elections.[99] And several of the largest tech companies and platforms, including Meta (Facebook and Instagram), Google (YouTube), and TikTok, have begun adopting or experimenting with labeling requirements for AI-generated content in various contexts, such as ads and deepfake media.[100]

Given this context, federal and state policymakers should focus their regulatory efforts on crafting effective transparency regimes for deepfakes and other synthetic content in political communications. To complement any general disclosure regime, policymakers should also consider targeted prohibitions on the most harmful kinds of deceptive content related to elections, such as content seeking to mislead voters on where, when, and how to vote, and potentially on certain types of content seeking to falsely cast doubt on the legitimacy of the electoral process. Finally, policymakers should enact targeted labeling regimes for a subset of content produced by LLMs, as well as for social media bots impersonating real or nonexistent humans when deployed by campaigns, parties, and others seeking to influence voters.

>> Mandate labels for political ads and similar communications containing deepfakes.

The best way to vindicate the public interest in an informed electorate without unduly burdening protected political speech is to require deepfakes and similar synthetically manipulated content to have labels informing viewers or listeners that the content has been manipulated. States including Arizona, California, Michigan, and Washington have pioneered legislation requiring disclaimers on certain fake video and audio content that inaccurately portray candidates seeking election.[101]

Federal and state lawmakers should also mandate watermarking technologies to ensure that AI-generated content can be identified even when it is shared or modified. The California AI Transparency Act is the nation's first law to mandate watermarking for AI-generated images, audio, and video. It requires creators to embed invisible signals to mark AI-produced content.[102] Future legislation should strengthen these rules by requiring that downstream users maintain the watermarking data to guarantee transparency throughout the entire life cycle of the content.

Deepfake rules should be tailored to avoid unnecessarily burdening expression. For example, a federal trial court recently enjoined an unduly broad California deepfake law that had some disclosure elements.[103] Whether or not this decision ultimately stands, there will still be much greater leeway under First Amendment precedents to require labeling of deepfakes and similar communications than to outright prohibit them.

Deepfake transparency rules should generally adhere to the following parameters:

- **Cover only substantially manipulated media.** When disclosure rules reach so broadly that virtually every communication requires a disclaimer, those disclaimers are rendered meaningless. Mandatory labels should be reserved for artificially generated or substantially modified visual and audio content that would leave a reasonable viewer or listener with a significantly different understanding of the speech or events depicted than those that actually occurred. This approach, though it might leave out some harmful content, is the best way to target the content most likely to deceive the public.

- **Include other manipulated content beyond deepfakes created through generative AI.** Many laws targeting manipulated content understandably focus on content generated or substantially modified using AI or generative AI. But a variety of digital methods for creating convincing audio and visual content do not require sophisticated technology, including basic photoshopping and video editing software. The best approach is to have uniform rules apply to all synthetically manipulated content that is likely to deceive reasonable members of the public.

- **Cover both audio and visual materials.** Audio deepfakes, such as those that targeted New Hampshire voters with a deepfake of President Biden's voice, are some of the easiest and most convincing fake content to produce. And yet audio deepfakes are sometimes omitted from deepfake disclosure rules — for instance, rules previously implemented by Meta for its various platforms (which have since been updated).[104]

- **Require short, easy-to-understand disclaimer language.** Disclaimers attached to manipulated content should be brief, direct, and accessible to a general audience. One example of an effective disclaimer is "This (image, video, or audio) has been manipulated."[105]

- **Target requirements at those creating and disseminating content to influence voters through paid advertising.** Disclosure requirements applicable to individuals and organizations creating or sharing content should focus on anyone clearly seeking to influence voters. Traditional campaign finance disclosure rules typically apply to candidates, parties, and political action committees (PACs), as well as others disseminating paid communications that plainly target voters.[106] Disclosure requirements should also cover individuals paid by campaigns, parties, and PACs that use AI-generated or deepfake content to influence voters. While such rules are not a perfect model for deepfake regulation, campaign finance rules offer an important precedent for requiring transparency from particular "speakers." In contrast, disclosure rules imposed on ordinary people speaking out on politics or any speaker focused solely on non-electoral public issues are more likely to be challenged.

- **Include reasonable requirements for online platforms and other tech companies.** Gaps in disclosure requirements for those creating and disseminating deceptive content can be filled partly by reasonable requirements for large online platforms. Existing proposed federal legislation would require these companies to maintain publicly accessible databases of their political ad sales.[107] Any such database should include information about whether an ad was generated or substantially modified by synthetic means. (The FCC recently proposed a similar rule for the public political ad files that television and radio broadcasters have long been required to maintain.[108]) Companies could also be required to use state-of-the-art tools to identify and label materially deceptive, digitally manipulated election content (including mechanisms for that content to be reported by affected parties). The California AI Transparency Act could provide a model in this regard.[109]

- **Craft appropriate exceptions.** Most enacted deepfake laws generally exempt some news media content. Some state rules also have carve-outs for content disseminated via broadcast television or radio, which are already subject to relatively comprehensive federal regulations.[110] There could be a case for exempting certain types of parody and satire; a California federal court, for instance, recently blocked a state law that would have required a disclaimer on a deepfake depicting Democratic presidential candidate Kamala Harris disparaging her own candidacy and record.[111] Many considered the deepfake depicting Harris to be satirical.[112] Regardless of whether the court's reasoning was correct, a well-crafted exemption might indeed have been appropriate, as satirical content poses less risk of deceiving voters.

>> Enact targeted deepfake prohibitions.

While disclosure is an effective tool for curbing most manipulated content, it is not a panacea. Not everyone who views or listens to deceptive content will notice a disclaimer. Video, images, and audio can still be altered to remove disclaimers, even with advances in watermarking technology. Disclaimer requirements can also be challenging to enforce in an era of microtargeted online ads. For these reasons, certain content that is especially harmful and has little to no redeeming value should be subject to targeted prohibitions, including content intended to mislead voters about where, when, or how to vote, as discussed in greater detail in the next section. Policymakers should also consider narrowly tailored prohibitions on content intended to falsely cast doubt on the legitimacy of the electoral process — for example, content purporting to depict illegal conduct related to the casting or counting of votes.

>> Require labeling of certain content produced by LLMs and social media bots.

Congress and state policymakers should require labeling for social media bots that impersonate real or nonexistent humans, as well as certain content produced by generative AI LLMs, including interactive chatbots, when deployed by candidates, parties, and PACs.

The use of generative AI chatbot technology in campaigns introduces serious risks for voters — of being peppered with falsehoods, of falling prey to promises or positions that fail to reflect a candidate's actual platform, and of unrestrained microtargeting based on problematic data collection. These risks are particularly pronounced when campaigns deploy generative AI technology to maintain continuous real-time interactions with voters or when AI-generated content is transmitted through AI bots that masquerade as humans.

Still more dangerous is the possibility that candidates, PACs, or those they direct will intentionally seek to deceive voters by conducting covert influence operations through personalized chatbots, robocalls, or other mechanisms — perhaps hiding such operations' connections to campaigns. Political agents could deploy generative AI chatbot technology to initiate interactive disinformation operations that can react in real time to voters, microtarget them based on sensitive demographic characteristics, and employ more sophisticated manipulation and persuasion techniques at scale.

To contend with these problems, Congress and state legislatures should require campaigns, PACs, and other core participants in the electoral process that deploy interactive chatbots and social media bots to advance their messages to label such content. These rules should target content transmitted

- through any interface or process capable of producing continuous interactions with voters by responding to their inputs and powered by an LLM or another kind of computer program; or

- through an automated software or automated process that impersonates authentic human activity on social media platforms, including by impersonating real or nonexistent humans.

Required disclaimers should, in plain language, inform the viewer or listener that the content was produced by a language-based generative AI system or software program, or that it reflects social media bot activity. In cases wherein social media bots share content substantially generated by AI, laws should require covered entities to disclose both that the account is a bot and that its content is produced by generative AI. As with deepfakes, disclaimers should be clearly visible and legible, or clearly comprehensible in the case of audio. Disclaimers should also be easily understood by those without technical backgrounds.

Even noninteractive content, such as bots posing as humans on social media to "like" campaign content and leave supportive or negative comments, can be harmful to the extent that it is used to deceive voters. When such social media accounts are maintained and content is produced by a campaign, party, or PAC, they too should be required to carry a straightforward label.

VI. Voter Suppression Prohibitions

Generative AI has the potential to supercharge voter suppression efforts, increasing their sophistication and their reach. Disinformation purveyors can now use AI tools to scale the production of falsehoods as basic as where, when, and how to vote. Building on a long and ignoble tradition of using deceptive practices to suppress American voters, the AI-generated impersonation of President Biden urging New Hampshire voters to sit out the 2024 presidential primary is a prime example of how urgently AI-augmented voter suppression efforts require government regulation.[113]

The spread of voter suppression deepfakes — AI-generated video and audio content that falsely depicts obstacles to voting, such as crises at polling centers, damage to voting equipment, and election officials obstructing voters — is a primary danger in today's electoral landscape. Those seeking to spread lies can also deploy LLMs, the technology underlying generative AI chatbots like ChatGPT and Gemini, to conduct thousands of deceptive real-time conversations with voters and fuel suppression.

Another voter suppression tactic in the United States with a long history is the wrongful purging of eligible voters from registration rolls.[114] AI can exacerbate these efforts to restrict the franchise. Most states allow activists to challenge a voter's registration status.[115] In current and prior election cycles, disinformation-fueled groups have filed frivolous voter challenges to try to strip tens of thousands of voters from the rolls.[116] In 2024, activists used at least one AI-assisted tool, EagleAI, to file meritless voter challenges more swiftly and easily, burdening election offices and putting voters at risk of disenfranchisement.[117] And developers have pitched this same flawed AI tool for use by election officials themselves. At least one county election board voted as early as December 2023 to buy EagleAI software to help identify voters to flag for potential removal from the rolls.[118] Policymakers should act swiftly to address these risks.

>> Toughen deceptive practice laws to better address AI risks.

Federal and state lawmakers should strengthen deceptive practices bills and laws to place stronger restraints on AI developers who intentionally disseminate AI tools to spread lies about the voting process. These laws and bills aim to address falsehoods about where, when, and how to vote. Lawmakers should improve them to account for the ease with which AI models can be taught to produce election deceptions through custom data sets of baseless election claims.[119] While lawmakers should also pass more fundamental reforms as previously discussed in this report, amending deceptive practices laws is an essential step.

Congress should first amend and pass the federal Deceptive Practices and Voter Intimidation Prevention Act, which would prohibit people from knowingly spreading material falsehoods about the time, place, or manner of elections within a 60-day period before a federal election with the intent to prevent or deter voting.[120] Several state legislatures (including Kansas, Minnesota, and Virginia) have enacted similar laws, while other states (including Michigan) have recently considered comparable legislation.[121] These existing deceptive practices laws and bills could be interpreted to cover some potential efforts by AI developers and deployers to spread election lies. But minor amendments could also ensure that legislation explicitly tackles more of the most worrisome ways that AI could exacerbate deceptive voter suppression practices.

To start, deceptive practices laws should expressly apply to AI developers whose actions to design AI tools or make them available for use result in the dissemination of falsehoods about where, when, and how to vote, when the developers intended to prevent or deter voting. But these laws should also extend liability to AI developers even if it cannot be proven that they knew that a specific claim generated by their tools was inaccurate, as long as they intended to suppress votes in designing and distributing the product. Deceptive practices laws typically require that those liable knew that the claim they spread or caused to be spread was false. While such a requirement makes good sense in most contexts, malevolent AI developers who aim to suppress votes should not be allowed to escape liability by claiming ignorance about the particular election facts that their tools undermine.

>> Prohibit the deliberate spread of deepfakes to suppress voting.

Lawmakers should specifically address the dissemination of deepfakes intended to suppress votes. As discussed above, the federal Deceptive Practices and Voter Intimidation Prevention Act would cover material falsehoods about the time and place of elections and rules on the conduct of elections, when spread to purposefully disenfranchise

voters.[122] The bill, which was first referred to committee in 2021 and has yet to receive a vote, would provide an important start for federal reform. Comparable laws have been enacted at the state level but are likewise limited. For example, Virginia's analogous law applies to "information . . . about the date, time, and place of the election, or the voter's precinct, polling place, or voter registration status, or the location of a voter satellite office or the office of the general registrar."[123]

Though such measures cover some AI-generated content, Congress and state legislatures should act to more comprehensively protect voters against potentially disenfranchising synthetic content. Such laws should prohibit the knowing distribution of digitally created or altered images, audio, or video files with the intent to prevent, impede, or deter a person from exercising their right to vote in the 60 days before an election, if the media contains content that falsely depicts

- defects of, vulnerabilities of, damage to, or impediments to the use of voting machines, ballots, ballot drop boxes, or other voting equipment;
- impediments to access to or use of polling places, including false depictions of emergencies at voting locations or physical obstacles to entry; or
- an officer holding an election or conducting a canvass, or another election worker, preventing or hindering an individual from voting.

Federal and state voter suppression deepfake laws should give affected voters and other aggrieved entities, such as voter assistance groups, a private right of action to civilly enforce such prohibitions, in addition to permitting enforcement by federal and state authorities. To protect voters in the time-sensitive period ahead of elections, these laws should require federal and state attorneys general to act to correct false information if election officials have been unable to adequately do so.

>> Strengthen regulation of political robocalls.

Policymakers should bolster regulation of political robocalls to address added dangers posed by generative AI. In February, the FCC clarified that it interprets existing statutory restrictions over robocalls containing "artificial or prerecorded voices" to extend to robocalls containing AI-generated content.[124] But federal law and regulations impose little restraint on political robocalls made to landlines, whether made using autodialing software, containing AI-generated voices, or both.[125] Americans over the age of 65 disproportionately use landlines, and they are also particularly vulnerable to deceptive voter suppression schemes.[126] Federal lawmakers should close this substantial loophole.

The FCC should also shore up regulation of AI-powered political robocalls so Americans can avoid receiving such calls unless they specifically consent to receiving AI-generated content. Existing law and regulations allow campaigns and others to make political robocalls to mobile devices using autodialing software, or to make calls containing AI-generated voices to mobile devices, if they obtain prior express consent.[127] Currently, however, consent is often inferred from voters' choice to give contact details to political campaigns, as long as they are informed that the campaign will use the information to conduct election outreach.[128] In August 2024, the FCC released details of a proposed rule that would require AI-generated robocall purveyors to clearly disclose in advance that a consumer's consent to receiving a robocall includes consent to receive AI-generated content.[129] The commission should issue a final rule with this requirement and clarify that it applies to political robocalls made to mobile devices as well as to commercial robocalls.

VII. Election Security Defenses

Artificial intelligence has the potential to introduce new and increased security threats for election offices and election system vendors alike. Because generative AI can excel at imitating authoritative sources, it will likely enable adversaries to more easily deceive voters as well as election workers by impersonating election officials or forging official election documents.

Foreign threat agents are exploring novel uses of AI in their attacks against the United States, according to U.S. intelligence agencies and technology companies.[130] Russian, North Korean, Iranian, and Chinese operations have been testing out LLMs for use in reconnaissance, translation, and phishing attacks.[131] As new AI technologies continue to become more accessible, those aiming to disrupt elections — including domestic antagonists — will undoubtedly seek to use these systems to advance their attacks.

AI could be used to threaten election operations in myriad ways. Malefactors could use it to build more advanced malware to outsmart current software security tools; mislead election workers into aiding cyberattacks and disrupting election administration; intimidate election workers to interfere with their work; and deceive the public by imitating election offices or other trusted sources about where, when, or how to vote, or about election results. The recommendations below offer guidance to Congress and the states as to how best to protect U.S. elections from AI-related security threats.

>> Provide more funding for basic election security.

As new AI developments heighten the risk of cyberattacks on election infrastructure, election officials need more resources and support to implement safeguards, mitigation measures, and security best practices. Although election security has markedly improved since 2016, the vast majority of local election offices still have little or no dedicated cybersecurity expertise and limited resources available to keep up with rapidly evolving security challenges. Meanwhile, federal funding for election security has diminished: In the four years leading up to the 2024 election, states received just a quarter of the $805 million in election security funding that Congress provided in the previous four years.[132] State and local election officials need more support to ramp up cybersecurity protections against new AI and other evolving cybersecurity threats.

One way that states can help supplement cybersecurity capacity in local election offices is through cyber navigator programs. These programs enable states to hire trained cybersecurity and election administration professionals to aid local officials in assessing the security of their systems, identifying potential vulnerabilities, and developing tailored strategies to mitigate risks.[133] At least seven states — Florida, Illinois, Iowa, Massachusetts, Michigan, Minnesota, and Ohio — have launched cyber navigator programs in recent years.[134] Illinois's program spends around $1.1 million annually for 10 state cybersecurity experts to support 102 counties.[135] Similar personnel support scaled nationwide would cost around $34 million annually.[136]

State and local election officials also need funding to upgrade outdated election infrastructure, implement cybersecurity protections, and purchase resources like paper ballots that can be used as backups in case technology fails.[137] Replacing outdated voting equipment alone would cost more than $200 million nationwide.[138] Congress and state legislatures must provide sufficient and consistent funding to ensure that election infrastructure can keep up with rising threats, allowing election officials to focus on new and evolving ones.

Finally, election officials need more training, education, and guidance on how to identify and mitigate AI security threats. Leading up to the 2024 presidential election, CISA led thousands of security assessments and trainings in election offices across the country, which included guidance on risks related to generative AI.[139] As AI's capacity advances, CISA needs further support and resources to continue this work, and states should look to supplement these efforts to reach more of the nearly 10,000 election officials nationwide.

>> Invest in the next generation of captcha for election offices.

One way that malign actors could disrupt the operations of election offices through AI is by filing huge numbers of Freedom of Information Act (FOIA) and other open records requests, or by creating mass AI-generated comments intended to mislead election officials about public sentiment and concerns. Over the past few years, election officials have addressed such attacks by integrating captcha systems and spam filters into their websites to prevent being overwhelmed by inauthentic feedback.[140] Today's captchas analyze user behavior and present users with tasks to confirm that they are human, such as click-

ing an "I'm not a robot" checkbox or sliding a puzzle piece until it fits into the correct spot on-screen.

Congress and state legislatures should provide election offices that have not yet incorporated reputable and accessible captcha programs into their public-facing websites with funds to do so. Lawmakers should also invest in a new generation of captcha systems that will maximize security, privacy, and accessibility as AI becomes more sophisticated at defeating existing captcha programs, and they should ensure that election offices have the resources to replace them as needed.

>> Fund tools to authenticate official election content.

As AI-generated images, audio, and video become more advanced and more prevalent, new tools are being developed to help protect against deepfakes and other inauthentic content. One of the most promising developments is content authenticity technology, including digital signatures — specific authenticity tools that can be used to apply verifiable signatures to official documents — which are being standardized.[141] State and federal agencies (starting with CISA at the federal level) should work with election offices to test and use these tools going forward.

As discussed earlier in this report with regard to watermarking technology, content authenticity (or content provenance) tools work by embedding information into an image, audio, or video file when it is first created. The data can include details like when and where the content originated and if it has been edited or modified in any way. This digital trail stays with the file so that anyone who views it can see its history and track when and how it was created and modified before it reached their screen.[142] If widely implemented and understood by users, these tools can help voters, the media, and the public at large identify the provenance of authentic content — including official content and AI-manipulated media that is embedded with accurate content authenticity information.[143] Some promising signs indicate that these tools will become more common in the future: Many of the world's leading tech companies have made voluntary commitments to the White House and the public to work to authenticate and disclose AI-generated content, particularly that which is used in elections.[144] In addition, the Coalition for Content Provenance and Authenticity (C2PA), a group of tech companies, media, and civil society organizations, has created an open standard for using these tools that most major tech companies and platforms have adopted.[145]

Future elections will provide election offices with an opportunity to pilot these tools. To do so most effectively, they will need the assistance of experts from agencies like CISA and their state-level equivalents, along with funding support to run effective public awareness campaigns to educate voters on how to locate and interpret provenance information included in official communications.

>> Invest in voter education programs to build resiliency against AI security threats.

State and local election officials, among other government offices, should launch voter education campaigns to prepare the public for AI-related challenges in the coming years. These campaigns can help voters identify authentic information coming from election offices and reaffirm election officials as authoritative sources of information on voting. Election officials should leverage advertising, earned media,[146] and social media to inform voters where they can go for official information and what to look for to determine that the information is authentic — including the .gov domain, official social media authenticators, official digital signatures, and official watermarks used on photo and video content.

Congress and state legislatures should provide funding to support such campaigns. In response to the Covid-19 pandemic in 2020, a group of 23 states used $65 million in private grants on voter education campaigns to reassure voters of safety measures and to inform them of available voting options leading up to the general election.[147] A similar nationwide campaign to inform voters about AI risks would cost $126 million.[148]

>> Require tougher election vendor security standards.

Just as election offices are likely to be targets of AI-enhanced security threats, election system vendors could be targeted as well.[149] The Brennan Center has previously detailed ways in which the federal government could mandate election security best practices — including stronger security and resilience planning for vendors in the elections space (comparable with that for vendors in other federal government sectors designated as critical infrastructure).[150] Such reforms should include the following core components:

- **Independent federal oversight of vendor security practices:** Whether conducted through the Election Assistance Commission (EAC), CISA, DHS (which recently published AI security guidelines for owners and operators of critical infrastructure), or another federal agency, independent government oversight of the security practices of private companies that provide critical election infrastructure is past due.[151]

- **Baseline standards to maintain security:** Any independent oversight regime should include baseline standards for election system vendors around cybersecurity best practices and the use of AI.[152]

- **Vendor certification:** The EAC, CISA, or DHS should establish a new federal certification program for election system vendors; the agency should be empowered to enforce vendors' compliance with the above-mentioned baseline standards.[153]

- **Ongoing review of security practices:** Oversight and regular monitoring of vendor security practices should be established to help ensure continued compliance with baseline standards.

Given the new threats to election security posed by AI, these calls for a new security framework to identify and address potential security risks posed by election security vendors and their use of AI could not be more urgent.[154]

At the national level, the EAC could execute some of the above recommendations without an additional congressional mandate as part of the registration and certification programs under its Voluntary Voting System Guidelines authorities.[155] Ideally, however, the challenge of election-related AI uses should be tackled in a more comprehensive way, through a mandate from Congress for the EAC or another federal agency to establish election security best practices for vendors, as Congress has done for vendors in other critical infrastructure sectors.[156]

VIII. Election Administration Standards

Artificial intelligence tools are becoming cheaper and more widely available, and private companies are rapidly deploying them to perform basic functions and increase productivity.[157] Under-resourced and understaffed election offices have every reason to do so as well. Indeed, in a survey of local election officials conducted by the Brennan Center in February and March of 2024, more than one in ten respondents reported that they had already been approached by private vendors with products advertised as using AI.[158]

In the not-too-distant future, election offices will likely be using AI to automate different processes, such as identifying new polling places, adjudicating ballots, generating translated materials, and analyzing postelection data to improve future elections.[159] No doubt, as AI technology continues to advance, new opportunities to optimize tasks and make election administration more efficient — especially in understaffed offices — will emerge.

Even with these potential benefits, however, AI-related risks and vulnerabilities cannot be overlooked. In 2017, DHS designated election systems as part of the country's critical infrastructure because of the vital role they play in sustaining American democracy.[160] Policymakers must work to identify and mitigate AI-related risks in election administration and to prevent unacceptable harms to voters, the election process, and electoral integrity overall.

Generative AI tools can help streamline tasks and summarize data, but they also have the potential for bias and hallucinations (the latter defined as outputs that make no sense or are entirely inaccurate). Newsfeeds trumpet innumerable examples of AI products failing or posing outsized security or privacy risks, amplifying biases, sharing hallucinated false information, and making other mistakes or reflecting vulnerabilities that human supervisors of the AI systems failed to catch.[161]

In many jurisdictions, election officials use AI-powered tools to maintain voter registration databases and verify mail ballot signatures, including detecting duplicate entries and analyzing handwriting patterns.[162] All of these are sensitive, rights-affecting uses. If implemented with appropriate guardrails, AI systems can improve election security, increase efficiency, and reduce the risk of eligible registrants being wrongfully purged from voter rolls or otherwise disenfranchised. Yet even otherwise legitimate AI systems are not impervious to error. And with the explosion of interest in AI by innovators and opportunists alike, unscrupulous vendors could shop dubious and error-prone AI systems to election officials.[163] In either case, election officials are not technical experts and may not fully understand AI systems' limitations; particularly when AI tools appear to be performing well, they may sometimes fail to recognize problems in time, or they may not see the need to institute important risk mitigations.

All of this comes at a time when public confidence in the American electoral system is already dangerously low, amplified by false claims made after the 2020 election.[164] Failures like these in crucial election functions could cause further, long-term damage to the public's faith in elections and, in the worst-case scenario, endanger the right to vote. Regulation is essential to safeguard the integrity of U.S. elections while still encouraging responsible innovation and embracing AI's potential election administration benefits.

Congress and the states should act now to institute governance mechanisms to mitigate these risks and develop processes to communicate to constituents when and how they use AI. As AI tools become integral to day-to-day election operations, federal and state agencies need to implement standards, certification, and monitoring regimes for their use in election offices, and for vendors selling AI products and services for use in election administration.

>> Create sector-specific guidance for election officials.

Election officials would undoubtedly appreciate government guidelines on whether and how to use AI in their work, yet no state legislators have introduced a bill that would provide such guidance in the last few sessions.[165] In contrast, at the federal level, Sens. Amy Klobuchar (D-MN) and Susan Collins (R-ME) put forth a bipartisan bill in March 2024 that would require the EAC to develop voluntary guidelines for AI use in election administration in federal elections.[166] The bill was voted out of the Senate Rules Committee last May but never came to the floor.[167]

Congress should take several immediate steps to help election officials who choose to integrate AI into their work do so as safely as possible:

- Provide funding for NIST to create an election-specific analogue to its *Artificial Intelligence Risk Management Framework*. In response to the Biden administration's

2023 AI executive order, NIST published its *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* in July 2024, but it was not specific to elections.[168] DHS also published safety and security guidelines for critical infrastructure owners and operators (integrating the NIST framework) in November 2024.[169] But guidelines customized for elections would help election officials better understand how to apply the general recommendations in NIST's *Artificial Intelligence Risk Management Framework* to circumstances particular to their work. Unique risks like voter disenfranchisement and other specific rights-affecting outcomes warrant circumspect, context-specific guidance, and election offices lack the resources and technical expertise to comprehensively identify sector-specific AI vulnerabilities and mitigations.

- Establish a standards and certification process to help election officials identify AI systems that meet baseline federal standards for use in election administration. These new standards must be augmented with a monitoring and auditing regime (discussed below) once systems are deployed to allow election offices and vendors to adjust how they use AI and ensure that risk-mitigation measures are as robust as possible.

- Dedicate funding for the EAC or CISA (or both in coordination) to build a centralized database for election officials and others to report AI-related incidents. The database should specifically include instances when AI-supported systems "unintentionally or maliciously" impeded election officials from fairly and efficiently administering elections, including by producing results that discriminated against particular classes of voters.[170]

- Allocate funds for state and local election offices to implement the relevant AI guidelines and standards both to administer elections and for the monitoring, auditing, and red-teaming of AI systems that will be necessary going forward.

While these recommendations are for Congress, state legislatures should adopt similar measures for election offices in their states. Additionally, at the federal level — even without congressional action — the EAC, CISA, and NIST should work together to establish administrative guidance on how to use AI in election administration with appropriate guardrails and to create a centralized incident reporting system for election officials and others to report AI-related harms.

>> Create an AI and Emerging Technologies Elections Lab to assist election officials.

AI and other future technologies promise to allow under-resourced election officials to serve the public more productively. To do so, election officials will need assistance in thinking through how these new technologies can best be deployed for various tasks, ideally from an entity dedicated to improving election administration and unconnected to private vendors with a financial interest in selling AI-related products. One way to provide such assistance would be for states and private donors to create an AI and Emerging Technologies Election Lab connected to a state educational institution that could work with state and local election officials to understand AI's potential applications in the elections space, develop ideas and products for election officials to pilot, and determine ways to comply with state guidance for using and auditing such products.

>> Mandate monitoring and auditing of AI tools used for election administration.

Congress should direct the relevant federal agencies to develop auditing protocols for specific sectors and require audits for high-risk AI uses, including administering elections. Detailed benchmarks for assessing AI tools' performance and vulnerabilities — such as baseline standards and metrics for adequate security, reliability, privacy, explainability and interpretability, resilience, protections against unacceptable bias, and appropriate risk mitigation — should be tailored to specific domains and uses. These benchmarks should be established in consultation with relevant expert officials. For election administration, Congress should direct expert officials to work with the EAC and CISA to institute audit AI protocols, including performance assessments across varied data sets and risk controls, along with red-teaming for security and other vulnerabilities. If Congress does not act, then states must take the lead in laying the groundwork.

Among other potential high-risk uses in election offices and at polling locations, federal and state lawmakers should require audits of

- AI systems intended for use to identify potentially ineligible voters or others who might be removed from voter rolls;

- AI systems intended for use to verify voters' identities; and

- AI systems used to provide important election information to voters, such as where polling places are located, hours of operation, and what forms of identification are required.

Lawmakers should require periodic reviews of AI systems by independent auditing bodies certified for following

election-specific AI auditing protocols. Self-certification by either AI vendors or election offices will not sufficiently guard against the significant risks to election systems and voting: AI vendors have been known to offer misleading descriptions of their products' reliability to election officials, and election offices lack the technical expertise and resources to comprehensively assess AI systems' performance and vulnerabilities.[171] Auditing bodies should have privileged access to the data they need to properly evaluate AI systems, with corresponding privacy protections and safeguards in place. They should also be required to submit audit results to appropriate federal-level government agencies (such as the EAC or CISA) for evaluation.

Based on audit results and the regulatory standards proposed here and throughout this report, federal officials should publish and periodically update a list of AI systems determined to be suitable for use in election administration for specified purposes and under stipulated conditions, as well as those unsuitable for use. States should refer to those lists and use those conditions as guidelines.

>> Limit the use of AI to manage voter rolls and purge or challenge voters.

Federal law already imposes hefty restrictions on voter roll purges, but additional safeguards are necessary to protect voters from baseless challenges and the misuse of AI in voter removal processes.[172] Congress and state legislatures should implement baseline standards for the use of AI systems to manage voter rolls and direct agencies to develop and update regulations as AI technologies advance. To prevent wrongful disenfranchisement, states should establish criteria for AI systems' security, explainability, privacy enhancements, accuracy, and reliability — and, relatedly, for the quality of the training data used in AI systems that support voter roll purges. Furthermore, all AI-assisted decisions to remove voters from the rolls should be subject to human review. Periodic independent audits should be required to assess the performance and vulnerabilities of any AI system used to update voter rolls.

The peril of unregulated and unreliable AI systems being used to challenge voters' eligibility should also force states to reexamine outdated voter challenge procedures.[173] In states where private citizens are permitted to challenge voter eligibility, lawmakers should institute protections against frivolous challenges, set clear documentation and evidence standards for valid challenges, and limit acceptable types of evidence.[174] Both federal and state lawmakers should prohibit the use of automated bots to file voter registration challenges with election offices. States should require private challenges to rely on firsthand knowledge of a voter's potential ineligibility, excluding the use of AI-driven or automated database-matching systems.

>> Regulate AI use to conduct signature matching.

A number of states require election offices to match the signature on a mail ballot envelope with the signature on file at the election office to safeguard the integrity of the ballot.[175] Many election offices already use non-generative AI to take the first pass at this time- and labor-intensive (and rights-affecting) task. Although the specific technology varies by vendor, ballots are generally fed through a scanner that captures an image of the signature and compares it with the signature on file.[176] Accuracy rates for AI-assisted signature matching fluctuate dramatically, and studies show that ballots from young, first-time mail-in voters, elderly voters, voters with disabilities, and nonwhite voters are more likely to be rejected.[177]

State lawmakers should help local election offices mitigate these risks when using AI for signature matching. One approach would be requiring that signature-matching systems include sufficient training data for the types of signatures that the software might struggle to validate, such as those mentioned above. Appropriate human review of flagged ballots should be mandatory, as should bipartisan team review of any ballot that has been flagged and team consensus before the ballot is rejected. In addition, states should compel election offices to notify voters and provide an opportunity to cure any issues concerning their signature. A number of states already follow such procedures.[178]

These processes are vital to ensuring that AI systems do not erroneously prevent voters from having their ballots counted. Election workers — especially those on the bipartisan teams that review flagged ballots — must understand AI tools' limitations or they risk being overly deferential to the systems' determinations. Moreover, ongoing independent audits of these systems' performance and processes can help verify that they continue to perform with a high level of accuracy and that biases are identified and adequately addressed before they cause irreparable harms.

Conclusion

That AI will alter American society is a foregone conclusion; indeed, it already has, and it will continue to in ways that are only starting to come into focus. What remains to be seen is how it will transform U.S. democracy — for better or for worse. To protect and preserve the future of democracy in America, policymakers must act now to ensure that these powerful tools are harnessed for pro-democracy ends.

This endeavor starts with building the governance institutions and frameworks to educate those adopting and deploying AI about its potential risks, and to empower them to support its implementation and use in the service of the American public and of democratic norms. That means that lawmakers must take every possible step to require those who profit from these new technologies to be transparent about how the tools they provide are being used, and to hold them accountable when those tools are employed to undermine Americans' ability to meaningfully participate in the democratic process.

When it comes to regulating AI in the elections space, one lesson from 2024 is that AI — and generative AI in particular — has the capacity to improve and streamline the procedures and processes that underlie our democratic elections, but also to amplify threats to electoral integrity that have long existed in the United States.[179] In 2024, AI was employed to spread election disinformation, suppress votes, and aid foreign government interference in U.S. elections. This kind of damaging use is almost certain to intensify as AI technologies evolve and become even more accessible.

While the reforms discussed in this report are necessary to constrain malefactors' ability to use AI systems to exploit any underlying weaknesses in American democracy — and also to incentivize those systems' pro-democracy uses — ultimately, the most important action that policymakers can take to protect democracy from the risks posed by AI is to tackle those weaknesses head-on. What the United States needs now is comprehensive democratic reform that provides Americans with a more open, more representative, more accountable, and more responsive system of government, one that preserves civil rights and liberties, privacy, and equality and is capable of withstanding whatever challenges the AI age may bring.

Endnotes

1 Galen Druke, "2024 Is the 1st 'AI Election.' What Does That Mean?," ABC News, December 1, 2023, https://abcnews.go.com/538/2024-1st-ai-election/story?id=105312571. AI refers to an expansive category of computer systems that leverage data, algorithms, and computational power to process information in ways that once only human intelligence could. Traditional AI tools can accomplish tasks like recognizing speech, identifying patterns in data, and making predictions. AI is now used in everyday applications from TV, film, and digital video recommendations to facial recognition for airport security to driving cars. The Organisation for Economic Co-operation and Development (OECD) has defined an AI system as a "machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." This report adopts that definition. See Organisation for Economic Cooperation and Development, "Explanatory Memorandum on the Updated OECD Definition of an AI System," OECD Artificial Intelligence Development Papers, no. 8, March 2024, https://doi.org/10.1787/623da898-en.

2 Emma Folts, "Voters: Here's How to Spot AI 'Deepfakes' That Spread Election-Related Misinformation," Heinz College, Carnegie Mellon University, October 18, 2024, https://www.heinz.cmu.edu/media/2024/October/voters-heres-how-to-spot-ai-deepfakes-that-spread-election-related-misinformation1; and Mike Wereschagin, "AI-Powered Deepfakes Threaten 'Chaos in the System' in Historic Election Year," *Pittsburgh Post-Gazette*, February 4, 2024, https://www.post-gazette.com/news/election-2024/2024/02/04/ai-deepfakes-fcc-chaos-presidential-election/stories/202402040088.

3 Zelly Martin et al., *Political Machines: Understanding the Role of Generative AI in the U.S. 2024 Elections and Beyond*, Center for Media Engagement, University of Texas at Austin, June 6, 2024, https://mediaengagement.org/research/generative-ai-elections-and-beyond; Marc Andreesen, "The Techno-Optimist Manifesto," Andreessen Horowitz, October 16, 2023, https://a16z.com/the-techno-optimist-manifesto; and Dave Karpf, "Parsing the Political Project of Techno-Optimism," Tech Policy Press, December 19, 2023, https://www.techpolicy.press/parsing-the-political-project-of-techno-optimism.

4 Juliana Kim, "Microsoft Detects Fake News Sites Linked to Iran Aimed at Meddling in U.S. Election," NPR, August 9, 2024, https://www.npr.org/2024/08/09/nx-s1-5069317/iran-interfere-presidential-election-microsoft-report; and Darren Linvill and Patrick Warren, "New Russian Disinformation Campaigns Prove the Past Is Prequel," *Lawfare*, January 22, 2024, https://www.lawfaremedia.org/article/new-russian-disinformation-campaigns-prove-the-past-is-prequel.

5 Shanze Hasan, "The Effect of AI on Elections Around the World and What to Do About It," Brennan Center for Justice, June 6, 2024, https://www.brennancenter.org/our-work/analysis-opinion/effect-ai-elections-around-world-and-what-do-about-it.

6 Jane C. Timm, "Inside the Right's Effort to Build a Voter Fraud Hunting Tool," NBC News, August 17, 2023, https://www.nbcnews.com/politics/2024-election/conservatives-voter-fraud-hunting-tool-eagleai-cleta-mitchell-rcna97327.

7 Maria Papageorgiou, "Social Media, Disinformation, and AI: Transforming the Landscape of the 2024 U.S. Presidential Political Campaigns," *The SAIS Review of International Affairs*, January 14, 2025, https://saisreview.sais.jhu.edu/social-media-disinformation-and-ai-transforming-the-landscape-of-the-2024-u-s-presidential-political-campaigns/.

8 Dean Jackson, Matthew Weil, and William T. Adler, *Preparing for Artificial Intelligence and Other Challenges to Election Administration: Results from Tabletop Exercises in Five States During the 2024 Election*, Bipartisan Policy Center, October 2024, https://bipartisanpolicy.org/report/preparing-for-artificial-intelligence-and-other-challenges-to-election-administration.

9 Nick Bilton, "Dizzying Deepfakes and Personalized Propaganda: Welcome to the AI Election," *Vanity Fair*, September 6, 2024, https://www.vanityfair.com/news/story/welcome-to-the-ai-election; Charlotte Hu, "How AI Bots Could Sabotage 2024 Elections Around the World," *Scientific American*, February 13, 2024, https://www.scientificamerican.com/article/how-ai-bots-could-sabotage-2024-elections-around-the-world; Nathan E. Sanders and Bruce Schneier, "AI Could Still Wreck the Presidential Election," *Atlantic*, September 24, 2024, https://www.theatlantic.com/technology/archive/2024/09/ai-election-ads-regulation/680010; Thalia Khan, "What Role Did AI Play in the 2024 U.S. Election?," Partnership on AI, November 4, 2024, https://partnershiponai.org/what-role-did-ai-play-in-the-2024-u-s-election; and "The First 'AI Elections' Weren't as Disastrous as Predicted. Here's Why," *Fast Company*, December 4, 2024, https://www.fastcompany.com/91239055/ai-2024-elections-politics.

10 Bruce Schneier, "How AI Will Change Democracy," *Schneier on Security* (blog), May 31, 2024, https://www.schneier.com/blog/archives/2024/05/how-ai-will-change-democracy.html.

11 Communications Decency Act of 1996, 47 U.S.C. § 230.

12 Administrative Procedure Act of 1946, 5 U.S.C. §§ 551–559.

13 Mekela Panditharatne, "Preparing to Fight AI-Backed Voter Suppression," Brennan Center for Justice, April 16, 2024, https://www.brennancenter.org/our-work/research-reports/preparing-fight-ai-backed-voter-suppression.

14 Graham Wilson and Maxwell Schechter, "The FCC Did Not Ban All AI Robocalls: Political Organizations Can Implement an AI Robocall Program with Certain Restrictions," Elias Law Group Newsroom, February 23, 2024, https://www.elias.law/newsroom/client-alerts/the-fcc-did-not-ban-all-ai-robocalls.

15 "AI Is Showing 'Very Positive' Signs of Eventually Boosting GDP and Productivity," Goldman Sachs, May 13, 2024, https://www.goldmansachs.com/insights/articles/AI-is-showing-very-positive-signs-of-boosting-gdp.

16 Lawrence Norden and Benjamin Lerude, "States Take the Lead on Regulating Artificial Intelligence," Brennan Center for Justice, November 6, 2023, https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence; and MultiState.ai, "States Studying AI," September 20, 2024, https://www.multistate.ai/states-studying-ai.

17 Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023), Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

18 Initial Rescissions of Harmful Executive Orders and Actions, Exec. Order (January 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions.

19 State of Georgia Technology Authority, "AI Advisory Council," accessed January 14, 2025, https://gta.georgia.gov/policies-and-

programs/artificial-intelligence/ai-advisory-council; Commonwealth of Massachusetts, "Governor Healey Signs Executive Order Establishing Artificial Intelligence (AI) Strategic Task Force," news release, February 14, 2024, https://www.mass.gov/news/governor-healey-signs-executive-order-establishing-artificial-intelligence-ai-strategic-task-force; Oregon State Enterprise Information Services, "State Government Artificial Intelligence Advisory Council," accessed January 14, 2025, https://www.oregon.gov/eis/pages/ai-advisory-council.aspx; and Tennessee Department of Finance and Administration, "Artificial Intelligence Advisory Council," accessed January 14, 2025, https://www.tn.gov/finance/ai-council.html.

20 Akin Gump Strauss Hauer & Feld LLP, "Louisiana's House Resolution 66 Created to Allow Joint Legislative Committee on Technology and Cybersecurity to Study Implications of AI," AI Law and Regulation Tracker, May 30, 2024, https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/louisianas-house-resolution-66-created-to-allow-joint-legislative-committee-on-technology-and-cybersecurity-to-study-implications-of-ai; and Resolution to Study Artificial Intelligence, H.R. 170, 2023–24 Sess. (Pa. 2024), https://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?syear=2023&sind=0&body=H&type=R&bn=170.

21 National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Cong. (2019–2020), https://www.congress.gov/bill/116th-congress/house-bill/6216; and AI.gov, "National AI Advisory Committee," accessed January 14, 2025, https://web.archive.org/web/20241231133912/https:/ai.gov/naiac.

22 Rebecca Heilweil and Madison Alder, "Here's Who's Responsible for AI in Federal Agencies," FedScoop, November 28, 2023, https://fedscoop.com/heres-whos-responsible-for-ai-in-federal-agencies.

23 Minnesota IT Services, "Minnesota's Intentional Approach to Artificial Intelligence," October 24, 2023, https://mn.gov/mnit/taiga/news.jsp?id=593353.

24 State of Utah Department of Commerce, "The Utah Department of Commerce Announces the Official Launch of the Utah Office of Artificial Intelligence Policy," July 8, 2024, https://blog.commerce.utah.gov/2024/07/08/the-utah-department-of-commerce-announces-the-official-launch-of-the-utah-office-of-artificial-intelligence-policy; and "Utah Launches Office of Artificial Intelligence Policy," *Government Technology*, July 10, 2024, https://www.govtech.com/artificial-intelligence/utah-launches-office-of-artificial-intelligence-policy.

25 Maya Kornberg and Martha Kinsella, *Building Science and Technology Expertise in Congress*, Brennan Center for Justice, November 6, 2023, https://www.brennancenter.org/our-work/policy-solutions/building-science-and-technology-expertise-congress.

26 Adaptation Clearinghouse, "National Academies of Sciences, Engineering, and Medicine (NASEM)," Georgetown Climate Center, accessed January 14, 2025, https://www.adaptationclearinghouse.org/organizations/national-academies-of-sciences-engineering-and-medicine-nasem.html.

27 Maya Kornberg, "To Be Effective on Tech, Congress Needs a Tech Committee," The Hill, November 22, 2022, https://thehill.com/opinion/technology/3746995-to-be-effective-on-tech-congress-needs-a-tech-committee.

28 Judy Schneider and Christopher M. Davis, *Reorganization of the House of Representatives: Modern Reform Efforts*, CRS report no. RL31835, Congressional Research Service, October 20, 2003, https://crsreports.congress.gov/product/pdf/RL/RL31835; and Judy Schneider et al., *Reorganization of the Senate: Modern Reform Efforts*, CRS report no. RL32112, Congressional Research Service, October 15, 2003, https://crsreports.congress.gov/product/pdf/RL/RL32112/4.

29 *Hearing on Oversight of AI: Rules for Artificial Intelligence*, 118th Cong. 118-037 (2023), https://www.govinfo.gov/app/details/CHRG-118shrg52706/CHRG-118shrg52706; *Hearing on Oversight of AI: Principles for Regulation*, 118th Cong. 118-108 (2023), https://www.govinfo.gov/app/details/CHRG-118shrg53503/CHRG-118shrg53503; *Hearing on AI and the Future of Our Elections*, 118th Cong. 118-130 (2023), https://www.govinfo.gov/app/details/CHRG-118shrg53678/CHRG-118shrg53678; and *Hearing on Addressing Real Harm Done by Deepfakes*, 118th Cong. 118-94 (2024), https://www.govinfo.gov/app/details/CHRG-118hhrg55181/CHRG-118hhrg55181.

30 Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023).

31 Shalanda D. Young, Office of Management and Budget (OMB) proposed memorandum re. advancing governance, innovation, and risk management for agency use of artificial intelligence (draft for public review), November 1, 2023, https://web.archive.org/web/20241231114255/https:/www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf.

32 For example, in 2024, California appropriated funding to its Government Operations Agency to coordinate the execution of Governor Gavin Newsom's 2023 AI executive order, one goal of which was a report on "the most significant, potentially beneficial use cases for deployment of GenAI tools by the state," as well as "potential risks to individuals, communities, and government and state government workers, with a focus on high-risk use cases." See Budget Act of 2024, A.B. 107, 2023–24 Sess. (Cal. 2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB107; and State of California Executive Department, Executive Order N-12-23, September 6, 2023, 3, https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12-_-GGN-Signed.pdf.

33 Utah AI Summit: Leading the Future of Artificial Intelligence, Salt Lake Community College Miller Campus, Salt Lake City, UT, October 30, 2024, https://ai.utah.gov/aisummit.

34 State of Utah Department of Commerce, "Utah Office of Artificial Intelligence Policy's Call for Public Suggestions on Next Learning Agenda," November 19, 2024, https://blog.commerce.utah.gov/2024/11/19/news-release-utah-office-of-artificial-intelligence-policys-call-for-public-suggestions-on-next-learning-agenda.

35 Young, "Advancing Governance."

36 "Make Your Voice Heard," AI.gov, September 26, 2024, https://web.archive.org/web/20240926223813/https://ai.gov/input.

37 Exec. Order No. 14179, 90 Fed. Reg. 8741 (2025), Removing Barriers to American Leadership in Artificial Intelligence, January 23, 2025, https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

38 Young, "Advancing Governance" (defining AI uses that can affect rights and safety).

39 Young, "Advancing Governance."

40 National Institute of Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, U.S. Department of Commerce, https://doi.org/10.6028/NIST.AI.100-1.

41 Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023); and NIST, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, U.S. Department of Commerce, July 2024, https://doi.org/10.6028/NIST.AI.600-1.

42 Department of Homeland Security (DHS), "Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security," news release, November 14, 2024, ; and DHS, *Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure*, November 14, 2024, https://www.dhs.gov/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure; and DHS, *Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure*, November 14, 2024, https://www.dhs.gov/sites/default/files/2024-11/24_1114_dhs_ai-roles-and-responsibilities-framework-508.pdf.

43 Jim Dempsey and Susan Landau, "Challenging the Machine: Contestability in Government AI Systems," *Lawfare*, https://www.lawfaremedia.org/article/challenging-the-machine-contestability-in-government-ai-systems.

44 Kim Lyons, "Pennsylvania Governor Creates Board to Oversee Use of Artificial Intelligence," the74million.org, October 2, 2023, https://www.the74million.org/article/pennsylvania-governor-creates-board-to-help-steer-states-use-of-generative-ai.

45 Fredrik Heiding, Bruce Schneier, and Arun Vishwanath, "AI Will Increase the Quantity — and Quality — of Phishing Scams," *Harvard Business Review*, May 30, 2024, https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams.

46 Mekela Panditharatne, Daniel I. Weiner, and Douglas Kriner, "Artificial Intelligence, Participatory Democracy, and Responsive Government," Brennan Center for Justice, November 3, 2023, https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-participatory-democracy-and-responsive-government.

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

48 See EUR-Lex, Regulation (EU) 2024/1689 (Artificial Intelligence Act, June 13, 2024), *Official Journal of the European Union*, July 12, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689; and EUR-Lex, Regulation (EU) 2022/2065 (Digital Services Act, October 19, 2022), *Official Journal of the European Union*, October 27, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065https://eur-lex.europa.eu/eli/reg/2022/2065/oj. See also EU Artificial Intelligence Act, "The AI Act Explorer," Future of Life Institute (FLI), accessed December 25, 2024, https://artificialintelligenceact.eu/ai-act-explorer; and European Parliament, "EU AI Act: First Regulation on Artificial Intelligence," last updated June 18, 2024, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

49 The EU AI Act defines such a system as "an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications." EU Artificial Intelligence Act, "High-Level Summary of the AI Act," FLI, last updated May 30, 2024, https://artificialintelligenceact.eu/high-level-summary (see "General Purpose AI (GPAI)"). EUR-Lex, Regulation (EU) 2024/1689 (Artificial Intelligence Act), recital 72, p. 21; and EUR-Lex, Regulation (EU) 2024/1689 (Artificial Intelligence Act), recital 107, p. 28.

50 *X Corp. v. Bonta*, 116 F.4th 888, 904 (9th Cir. 2024); *Moody v. NetChoice LLC*, 144 S. Ct. 2383, 2398 (2024); and *NetChoice LLC v. Paxton*, 142 S. Ct. 1715 (2022).

51 *Moody*, 144 S. Ct. at 2398.

52 EUR-Lex, Regulation (EU) 2024/1689 (Artificial Intelligence Act), ch. 1, art. 3, pt. 63, p. 50; and EUR-Lex, Regulation (EU) 2024/1689 (Artificial Intelligence Act), ch. 1, art. 3, pt. 66, p. 50.

53 These are more accurate terms than *open-source* for this usage. See Shakeel Hashim, "Lawrence Lessig Is Very Worried About Freely Available AI Model Weights," *Transformer*, July 2, 2024, https://www.transformernews.ai/p/lawrence-lessig-open-source-ai-risks.

54 EUR-Lex, Regulation (EU) 2022/2065 (Digital Services Act), ch. 3, § 5, art. 33, p. 63; and European Commission, "Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines," news release, April 24, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413.

55 EUR-Lex, Regulation (EU) 2022/2065, (Digital Services Act), ch. 3, § 5, art. 34, p. 64.

56 EUR-Lex, Regulation (EU) 2022/2065, (Digital Services Act), ch. 3, § 5, art. 35, p. 65.

57 EUR-Lex, Regulation (EU) 2022/2065, (Digital Services Act), ch. 3, § 5, art. 37, p. 67.

58 EUR-Lex, Regulation (EU) 2022/2065, (Digital Services Act), ch. 3, § 5, art. 40, p. 70.

59 Public Citizen, "Tracker: State Legislation on Deepfakes in Elections," last updated January 13, 2025, https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections.

60 Joel Simon, "Can AI Be Sued for Defamation?," *Columbia Journalism Review*, March 18, 2024, https://www.cjr.org/analysis/ai-sued-suit-defamation-libel-chatgpt-google-volokh.php.

61 For a look at existing state laws that address regulating AI in U.S. elections, see Lawrence Norden, Niyati Narang, and Laura J. Protzmann, "States Take the Lead in Regulating AI in Elections — Within Limits," Brennan Center for Justice, August 7, 2024, https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits.

62 See Alice Xiang, "Fairness and Privacy in an Age of Generative AI," *The Columbia Science and Technology Law Review* 25, no. 288 (Spring 2024): 288–312 (see esp. 301–4), https://journals.library.columbia.edu/index.php/stlr/article/view/12765/6289 (discussing the scope of Section 230 and its applicability to generative AI developers).

63 Communications Decency Act, 47 U.S.C. § 230.

64 Communications Decency Act, 47 U.S.C. § 230(f)(2)–(3) (defining interactive service providers and information content providers).

65 *Fair Housing Council v. Roommates.com*, 521 F.3d 1157, 1168 (9th Cir. 2008).

66 Congressional Research Service, "Section 230 Immunity and Generative Artificial Intelligence," December 28, 2023, https://crsreports.congress.gov/product/pdf/LSB/LSB11097.

67 Graham H. Ryan, "Generative AI Will Break the Internet: Beyond Section 230," *Harvard Journal of Law and Technology* 37 (Spring 2024): 14–15, https://jolt.law.harvard.edu/assets/digestImages/Generative-AI-Will-Break-the-Internet_-Beyond-Section-230-Final-Review.pdf.

68 S. 1993, 118th Cong., 1st Sess. (2023–24), https://www.congress.gov/bill/118th-congress/senate-bill/1993.

69 Jennifer King and Caroline Meinhardt, "Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World," Stanford University Human-Centered Artificial Intelligence White Paper, February 2024, https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

70 David Gilbert, "Election Deniers Are Ramping Up Efforts to Disenfranchise US Voters," *Wired*, July 31, 2024, https://www.wired.com/story/election-deniers-efforts-disenfranchise-voters.

71 Cade Metz et al., "How Tech Giants Cut Corners to Harvest Data for A.I.," *The New York Times*, April 8, 2024, https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html; and Stuart Madnick, "Why Data Breaches Spiked in 2023," *Harvard Business Review*, February 19, 2024, https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

72 The availability of a voter's file and confidential information will vary by state. See National Conference of State Legislatures, "Access to and Use of Voter Registration Lists," last updated October 7, 2024, https://www.ncsl.org/elections-and-campaigns/access-to-and-use-of-voter-registration-lists (listing voter file access laws by state).

73 California Privacy Rights Act of 2020, Cal. Civ. Code § 1798. §

1798.199.90 (2020), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1194; and Secure Privacy, "The Difference Between Opt-In vs Opt-Out Principles in Data Privacy: What You Need To Know," *Cookie Consent* (blog), February 1, 2024, https://secureprivacy.ai/blog/difference-beween-opt-in-and-opt-out.

74 Pandittharatne et al., "Artificial Intelligence, Participatory Democracy, and Responsive Government."

75 Issie Lapowsky, "How Bots Broke the FCC's Public Comment System," *Wired*, November 28, 2017, https://www.wired.com/story/bots-broke-fcc-public-comment-system.

76 Sarah Kreps and Douglas L. Kriner, "The Potential Impact of Emerging Technologies on Democratic Representation: Evidence from a Field Experiment," *New Media and Society* 26, no. 12, (December 2024): 6918–37.

77 Federal Trade Commission (FTC), "Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials," news release, August 14, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials.

78 Administrative Procedure Act, 5 U.S.C. §§ 551–559; and Nina A. Mendelson, "Foreword: Rulemaking, Democracy, and Torrents of E-mail," *The George Washington Law Review* 79, no. 5 (July 2011): 1343–80, https://www.gwlr.org/wp-content/uploads/2012/08/79-5-Mendelson.pdf.

79 Congressional Management Foundation, "Improve Mail Operations," accessed January 14, 2025, https://www.congressfoundation.org/news/110-mail-operations.

80 Katherine Levine Einstein and David M. Glick, "Does Race Affect Access to Government Services? An Experiment Exploring Street-Level Bureaucrats and Access to Public Housing," *American Journal of Political Science* 61, no. 1 (January 2017): 100–16.

81 Administrative Procedure Act, 5 U.S.C. §§ 551–559.

82 Mark Toner, "Government Wants Some Straight Talk About Chatbots," *Governing*, August 18, 2020, https://www.governing.com/next/government-wants-some-straight-talk-about-chatbots.html.

83 Thomas Kalil and David Wilkinson, "Harnessing the Power of Feedback Loops," *White House Blog*, January 3, 2017, https://obamawhitehouse.archives.gov/blog/2017/01/03/harnessing-power-feedback-loops.

84 Colin Wood, "To Test Emerging Tech Like AI, Georgia Plans Innovation Lab," StateScoop, May 9, 2024, https://statescoop.com/georgia-ai-innovation-lab-2024.

85 Mike Williams, "Transforming How New York Protects and Serves Its Community," Google Cloud, April 25, 2024, https://cloud.google.com/blog/topics/public-sector/transforming-how-new-york-protects-and-serves-its-community.

86 City of Charleston, South Carolina, "[Archived] City of Charleston Launches Citibot," July 8, 2020, https://www.charleston-sc.gov/CivicAlerts.aspx?AID=865&ARC=1692; and Citibot, "Building Multilanguage AI-Powered Chatbots to Foster Trust Between Governments and Residents," accessed January 14, 2025, https://www.citibot.io.

87 Aleksandra Wrona, "Does Pic Show Trump and Epstein with Minor Girl?," Snopes, January 9, 2024, https://www.snopes.com/fact-check/epstein-trump-young-girl-photo; and Rhian Lubin, "X Users Play Elon Musk at His Own Game After He Posts AI Image of Harris as Communist Dictator," *The Independent*, September 4, 2024, https://www.the-independent.com/news/world/americas/us-politics/elon-musk-harris-trump-communist-ai-x-b2606199.html.

88 Maggie Astor, "Behind the A.I. Robocall That Impersonated Biden: A Democratic Consultant and a Magician," *The New York Times*, February 29, 2024, https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html.

89 Julie Kay, "'It Should Be Used for the Truth': Fully AI-Generated Political Ad Parodies Lt. Gov. Mark Robinson's Campaign," WCNC (Charlotte, NC), September 24, 2024, https://www.wcnc.com/article/news/politics/north-carolina-politics/ai-generated-mark-robinson-parody-ad-9-24-2024/275-a7225cbb-b80f-426b-8341-f1b9f0ae0bc5.

90 Morgan Meaker, "Slovakia's Election Deepfakes Show AI Is a Danger to Democracy," *Wired*, October 3, 2023, https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy; Marianna Spring, "X Takes Action on Deepfake Network Smearing UK Politicians After BBC Investigation," BBC, June 8, 2024, https://www.bbc.com/news/articles/cq55gd8559eo; and Rishi Iyengar, "How China Exploited Taiwan's Election — and What It Could Do Next," *Foreign Policy*, January 23, 2024, https://foreignpolicy.com/2024/01/23/taiwan-election-china-disinformation-influence-interference.

91 Michael Crowley, Valerie Hopkins, and Edward Wong, "Deepfake of U.S. Official Appears After Shift on Ukraine Attacks in Russia," *The New York Times*, May 31, 2024, https://www.nytimes.com/2024/05/31/us/politics/deepfake-us-official-russia.html.

92 Mathias Hammer, "Belarusian Opposition Endorses AI Candidate in Parliamentary Elections," Semafor, February 23, 2024, https://www.semafor.com/article/02/23/2024/belarusian-opposition-endorses-ai-candidate.

93 Yan Zhuang, "Imran Khan's 'Victory Speech' from Jail Shows A.I.'s Peril and Promise," *The New York Times*, February 11, 2024, https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html.

94 *Citizens United v. FEC*, 558 U.S. 310, 366 (2010).

95 Norden et al., "States Take the Lead in Regulating AI in Elections."

96 Defending Democracy from Deepfake Deception Act of 2024, A.B. 2655, 2023–24 Sess. (Cal. 2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2655.

97 See, e.g., H.F. 1370, 2023–24 Sess. (Minn. 2024), https://www.revisor.mn.gov/bills/textphp?number=HF1370&type=bill&version=3&session=ls93&session_year=2023&session_number=0; H.F. 4772, 2023–24 Sess. (Minn. 2024), https://www.revisor.mn.gov/bills/text.php?number=HF4772&type=bill&version=1&session=ls93&session_year=2024&session_number=0; and S.B. 751, 2019–20 Sess. (Tex. 2019), https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm.

98 Brennan Center for Justice, "Artificial Intelligence Legislation Tracker," last updated December 30, 2024, https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-legislation-tracker.

99 See generally EU Artificial Intelligence Act, "AI Act Explorer."

100 Katie Paul, "Meta to Start Labeling AI-Generated Images from Companies Like OpenAI, Google," Reuters, February 6, 2024, https://www.reuters.com/technology/meta-start-labeling-ai-generated-images-companies-like-openai-google-2024-02-06; Ben Wodecki Jr., "YouTube Requires Users to Label AI-Generated Content," AI Business, March 20, 2024, https://aibusiness.com/responsible-ai/youtube-requires-users-to-label-ai-generated-content; and Andrew Hutchinson, "TikTok Adds New Required Labels for AI-Generated Content," Social Media Today, August 9, 2023, https://www.socialmediatoday.com/news/tiktok-adds-new-required-labels-for-ai-generated-content/690454.

101 Elections: Deceptive Audio or Visual Media, A.B. 730, 2019–20 Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730; Defining Synthetic Media in Campaigns for Elective Office, and Providing Relief for Candidates and Campaigns, S.B. 5152, 2023–24 Sess. (Wash. 2024), https://app.leg.wa.gov/billsummary/?billNumber=5152&year=2023&initiative=False; Regulate Use of Artificial Intelligence for Political Campaigns, H.B. 5141–5145, 2023–24 Sess. (Mich. 2023), https://legislature.mi.gov/

documents/2023-2024/billanalysis/House/pdf/2023-HLA-5141-6D54E9B1.pdf; and S.B. 1359, 2023–24 Sess. (Ariz. 2024), https://azleg.gov/legtext/56leg/2R/bills/SB1359S.pdf.

102 California AI Transparency Act, S.B. 942, 2023–24 Sess. (Cal. 2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942. See also Arsen Kourinian, Howard W. Waltzman, and Mickey Leibner, "New California Law Will Require AI Transparency and Disclosure Measures," Mayer Brown, September 23, 2024, https://www.mayerbrown.com/en/insights/publications/2024/09/new-california-law-will-require-ai-transparency-and-disclosure-measures.

103 See Alan Riquelmy, "Federal Judge Stops Implementation of California Misinformation Law," Courthouse News Service, October 2, 2024, https://www.courthousenews.com/federal-judge-stops-implementation-of-california-misinformation-law.

104 Monika Bickert, "Our Approach to Labeling AI-Generated Content and Manipulated Media," Meta, last updated September 12, 2024, https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media.

105 N.Y. Elec. Law § 14-106(5)(b)(ii)(1).

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

107 Tim Lau, "The Honest Ads Act Explained," Brennan Center for Justice, January 17, 2020, https://www.brennancenter.org/our-work/research-reports/honest-ads-act-explained.

108 Federal Communications Commission (FCC), "FCC Proposes Disclosure for AI-Generated Content in Political Ads," news release, July 25, 2024, https://www.fcc.gov/document/fcc-proposes-disclosure-ai-generated-content-political-ads. See also Daniel I. Weiner, Eric Petry, and Yasmin Abusaif, "Comment to the FCC: Embrace Greater Transparency by Requiring On-Air and Written Disclosures of AI-Generated and Synthetic Content in Radio and Television Political Advertisements," Brennan Center for Justice, September 19, 2024, https://www.brennancenter.org/our-work/research-reports/comment-fcc-embrace-greater-transparency-requiring-air-and-written-0.

109 California AI Transparency Act, S.B. 942 (Cal. 2024).

110 Elections: Deceptive Media in Advertisements, A.B. 2839, 2023–24 Sess. (Cal. 2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2839; Defending Democracy from Deepfake Deception Act, A.B. 2655 (Cal. 2024); Freedom From AI-Rigged (FAIR) Elections Act, H.B. 664, 2nd Reg. Sess., 2024 (Idaho 2024), https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2024/legislation/H0664.pdf; and H.F. 4772, 2023–24 Sess. (Minn. 2024), https://www.revisor.mn.gov/bills/text.php?number=HF4772&type=bill&version=1&session=ls93&session_year=2024&session_number=0.

111 *Kohls v. Bonta,* No. 2:24-CV-02527 JAM-CKD, 2024 WL 4374134, at *5 (E.D. Cal. Oct. 2, 2024) ("Supreme Court precedent illuminates that while a well-founded fear of a digitally manipulated media landscape may be justified, this fear does not give legislators unbridled license to bulldoze over the longstanding tradition of critique, parody, and satire protected by the First Amendment.").

112 Ali Swenson, "A Parody Ad Shared by Elon Musk Clones Kamala Harris' Voice, Raising Concerns About AI in Politics," Associated Press, July 29, 2024, https://apnews.com/article/parody-ad-ai-harris-musk-x-misleading-3a5df582f911a808d34f68b766aa3b8e.

113 Astor, "Behind the A.I. Robocall That Impersonated Biden."

114 Equal Justice Initiative, "Voter Suppression Persists Through Purging," July 23, 2018, https://eji.org/news/voter-suppression-persists-through-purging.

115 See Alice Clapman, "Attacks on Voter Rolls and How to Protect Them," Brennan Center for Justice, March 11, 2024, https://www.brennancenter.org/our-work/research-reports/attacks-voter-rolls-and-how-protect-them. See also Kevin Morris et al., *Purges: A Growing Threat to the Right to Vote*, Brennan Center for Justice, July 20, 2018, https://www.brennancenter.org/our-work/research-reports/purges-growing-threat-right-vote.

116 Alice Clapman and Mekela Panditharatne, "Four New Initiatives Driving Mass Voter Challenges," Brennan Center for Justice, July 22, 2024, https://www.brennancenter.org/our-work/research-reports/four-new-initiatives-driving-mass-voter-challenges; and Katie Friel et al., "'Citizen Integrity' Teams' Efforts Could Be Groundwork for Next False Claims About Election Results," Brennan Center for Justice, November 4, 2022, https://www.brennancenter.org/our-work/research-reports/citizen-integrity-teams-efforts-could-be-groundwork-next-false-claims.

117 Alice Clapman, "Florida's Use of Unreliable Tool Could Wrongly Remove Numerous Voters from Rolls," Brennan Center for Justice, May 31, 2024, https://www.brennancenter.org/our-work/analysis-opinion/floridas-use-unreliable-tool-could-wrongly-remove-numerous-voters-rolls.

118 Board of Commissioners, Columbia County, GA, memorandum to American Oversight re. open records request, "Agreement Between EagleAI and Columbia County, Ga," March 1, 2024, https://www.documentcloud.org/documents/24476343-ga-columbia-24-0175-a-processed-clean; and Mark Niesse, "Private Voter Verification Tech Approved in Republican Georgia County," December 14, 2023, *The Atlanta Journal-Constitution*, https://www.ajc.com/politics/georgia-county-agrees-to-use-eagleai-to-check-voter-registrations/EIEPKQOIDFG5JMZNUETJV7267Q.

119 Jeremy White, "See How Easily A.I. Chatbots Can Be Taught to Spew Disinformation," *The New York Times*, May 19, 2024, https://www.nytimes.com/interactive/2024/05/19/technology/biased-ai-chatbots.html.

120 Deceptive Practices and Voter Intimidation Prevention Act of 2021, S. 1840, 117th Cong. (2021–22), https://www.congress.gov/bill/117th-congress/senate-bill/1840/text.

121 Kan. Admin. Regs. § 25-2415 (2012), https://www.ksrevisor.org/statutes/chapters/ch25/025_024_0015.html; Minn. R. 204C.035 (2006), https://www.revisor.mn.gov/statutes/cite/204C.035; 313 Va. Admin. Code § 24.2-1005.1 (2007), https://law.lis.virginia.gov/vacode/title24.2/chapter10/section24.2-1005.1; and S.B. 707, 2023–24 Sess. (Mich. 2024), https://www.legislature.mi.gov/documents/2023-2024/billintroduced/Senate/pdf/2024-SIB-0707.pdf.

122 Deceptive Practices and Voter Intimidation Prevention Act of 2021, S. 1840, 117th Cong. (2021–22).

123 313 Va. Admin. Code § 24.2-1005.1(A) (2007).

124 Ali Swenson, "FCC Bans AI-Generated Voices in Robocalls That Can Deceive Voters," PBS News, February 8, 2024, https://www.pbs.org/newshour/politics/fcc-bans-ai-generated-voices-in-robocalls-that-can-deceive-voters.

125 Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227; FCC, "Political Campaign Robocalls and Robotexts Rules," October 22, 2024, https://www.fcc.gov/rules-political-campaign-calls-and-texts; and Wilson and Schechter, "FCC Did Not Ban All AI Robocalls."

126 Andrew Van Dam, "Barely a Quarter of Americans Still Have Landlines. Who Are They?," *The Washington Post*, June 23, 2023, https://www.washingtonpost.com/business/2023/06/23/landline-telephone-holdouts; and Nadia M. Brashier and Daniel L. Schacter, "Aging in an Era of Fake News," *Current Directions in Psychological Science* 29, no. 3 (June 2020): 316–23, https://pmc.ncbi.nlm.nih.gov/articles/PMC7505057/pdf/nihms-1628117.pdf.

127 FCC, "Political Campaign Robocalls and Robotexts Rules."

128 Michele Shuster, "TCPA Compliance for Political Calls,"

MacMurray and Shuster LLP, September 9, 2020, https://mslawgroup.com/tcpa-compliance-for-political-calls. (TCPA is short for the Telephone Consumer Protection Act, which Congress enacted in 1991 to restrict telemarketing calls and the use of automatic dialers and artificial or prerecorded voice messages. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227. In collaboration with the FTC, the FCC revised TCPA rules in 2003 to establish the national Do-Not-Call registry. The FCC revised TCPA rules again in 2012 to offer consumers more protections from telemarketers and robocalling. FCC, "FCC Actions on Robocalls, Telemarketing," last updated July 23, 2018, https://www.fcc.gov/general/telemarketing-and-robocalls.)

129 FCC, In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, CG Docket No. 23-362, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 24-84 (August 7, 2024), https://docs.fcc.gov/public/attachments/FCC-24-84A1.pdf.

130 U.S. Federal Bureau of Investigation, Department of Justice et al., "State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity," Joint Cybersecurity Advisory, Internet Crime Complaint Center (IC3), July 9, 2024, https://www.ic3.gov/media/news/2024/240709.pdf; U.S. Department of Justice et al., "Iran-Based Cyber Actors Enabling Ransomware Attacks on US Organizations," Joint Cybersecurity Advisory, IC3, August 28, 2024, https://www.ic3.gov/CSA/2024/240828.pdf; Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI," Microsoft, February 14, 2024, https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai; and Derek B. Johnson, "OpenAI Says It Has Disrupted 20-Plus Foreign Influence Networks in Past Year," CyberScoop, October 9, 2024, https://cyberscoop.com/openai-threat-report-foreign-influence-generative-ai.

131 Intel471, "Cybercriminals and AI: Not Just Better Phishing," June 12, 2024, https://intel471.com/blog/cybercriminals-and-ai-not-just-better-phishing.

132 Derek Tisler, "States Must Take the Lead on Election Security," Brennan Center for Justice, December 19, 2024, https://www.brennancenter.org/our-work/research-reports/states-must-take-lead-election-security.

133 CISA, "CISA Hosts Election Cybersecurity Navigators Forum for State and Local Election Officials," press release, December 21, 2021, https://www.cisa.gov/news-events/news/cisa-hosts-election-cybersecurity-navigators-forum-state-and-local-election.

134 Matt Vasilogambros, "States Use 'Cyber Navigators' for Foreign Election Threats," *Government Technology*, August 27, 2021, https://www.govtech.com/security/states-use-cyber-navigators-for-foreign-election-threats.

135 The Elections Group, "Illinois' Cyber Navigator Program," March 21, 2023, https://electionsgroup.com/resource/illinois-cyber-navigator-program.

136 Providing similar support nationwide would require 308 staff experts to support America's 3,143 counties and county equivalents and would cost $110,000 per staff expert annually. See U.S. Census Bureau, "County Population Totals and Components of Change: 2020–2023," last updated June 25, 2024, https://www.census.gov/data/tables/time-series/demo/popest/2020s-counties-total.html.

137 Edgardo Cortés et al., *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials*, Brennan Center for Justice, December 19, 2019, https://www.brennancenter.org/our-work/policy-solutions/preparing-cyberattacks-and-technical-failures-guide-election-officials.

138 Ruby Edlin, Megan Maier, and Warren Stewart, "Costs for Replacing Voting Equipment in 2024," Brennan Center for Justice, February 7, 2024, https://www.brennancenter.org/our-work/analysis-opinion/costs-replacing-voting-equipment-2024.

139 CISA, "Risk in Focus: Generative A.I. and the 2024 Election Cycle," January 18, 2024, https://www.cisa.gov/sites/default/files/2024-05/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf.

140 CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, is a common security measure intended to deter nefarious bots and other spam attacks. See Chas Newkey-Burden, "Why Captchas Are Getting Harder to Solve," *The Week*, April 28, 2024, https://theweek.com/tech/why-captchas-are-getting-harder-to-solve.

141 NIST, "Digital Signature Standard (DSS)," U.S. Department of Commerce, February 3, 2023, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.

142 Jim Thacker, "Adobe Announces New Content Authenticity Web App," CG Channel, October 8, 2024, https://www.cgchannel.com/2024/10/adobe-announces-new-content-authenticity-web-app.

143 Mekela Panditharatne and Shanze Hasan, "How to Detect and Guard Against Deceptive AI-Generated Election Information," Brennan Center for Justice, May 16, 2024, https://www.brennancenter.org/our-work/research-reports/how-detect-and-guard-against-deceptive-ai-generated-election-information.

144 Munich Security Conference, "A Tech Accord to Combat Deceptive Use of AI in 2024 Elections," February 16, 2024, https://securityconference.org/en/aielectionsaccord/accord.

145 Coalition for Content Provenance and Authenticity (CP2A), "Overview," accessed January 13, 2025, https://c2pa.org.

146 Earned media refers to publicity or exposure gained through unpaid methods. Unlike paid advertisements, earned media is generated through organic means, and its coverage can include anything from a feature on a news site to a mention on a social media post.

147 Center for Election Innovation and Research, "CEIR 2020 Voter Education Grant Program," March 26, 2021, https://electioninnovation.org/research/ceir-2020-voter-education-grant-program.

148 Those 12 states spent an average of $0.61 per active registered voter. The total estimate multiplies this per-voter cost by all active registered voters nationwide. U.S. Election Assistance Commission (EAC), *Election Administration and Voting Survey 2020: Comprehensive Report*, August 2021, https://www.eac.gov/sites/default/files/document_library/files/2020_EAVS_Report_Final_508c.pdf.

149 Pam Fessler and Philip Ewing, "Report: Russia Launched Cyberattack on Voting Vendor Ahead of Election," *All Things Considered* (NPR), June 5, 2017, https://www.npr.org/2017/06/05/531649602/report-russia-launched-cyberattack-on-voting-vendor-ahead-of-election.

150 Lawrence Norden, Gowri Ramachandran, and Christopher Deluzio, *A Framework for Election Vendor Oversight*, Brennan Center for Justice, November 12, 2019, https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight.

151 DHS, *Mitigating Artificial Intelligence (AI) Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators*, April 2024, https://dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf.

152 CISA, "Cybersecurity Toolkit and Resources to Protect Elections," accessed January 14, 2024, https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections; and Norden et al., *Framework for Election Vendor Oversight*.

153 Norden et al., *Framework for Election Vendor Oversight*.

154 Lawrence Norden and Gowri Ramachandran, "Artificial Intelligence and Election Security," Brennan Center for Justice, October 5, 2023, https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-and-election-security.

155 Norden et al., *Framework for Election Vendor Oversight*, 7.

156 Norden et al., *Framework for Election Vendor Oversight*, 4.

157 Nihal Krishan, "Federal Gov Spending on AI Hit $3.3B in Fiscal 2022: Study," FedScoop, April 17, 2023, https://fedscoop.com/us-spending-on-ai-hit-3-3b-in-fiscal-2022; and Kate Den Houter, "AI in the Workplace: Answering 3 Big Questions," Gallup, October 8, 2024, https://www.gallup.com/workplace/651203/workplace-answering-big-questions.aspx.

158 Brennan Center for Justice, "Local Election Officials Survey," May 1, 2024, https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-may-2024.

159 Devan Cole, "Here's What to Know About Ballot Adjudication," CNN, November 5, 2020, https://www.cnn.com/2020/11/05/politics/ballot-adjudication-explained/index.html.

160 Congressional Research Service, "The Designation of Election Systems as Critical Infrastructure," September 18, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10677; and EAC, "Elections — Critical Infrastructure," March 11, 2022, https://www.eac.gov/election-officials/elections-critical-infrastructure.

161 Bret Greenstein, Ege Gürdeniz, and Ilana Golbin, "AI Hallucinations: What Business Leaders Should Know," PWC, June 18, 2024, https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-hallucinations.html.

162 Sebastian Griffin, "The Good and the Bad of Artificial Intelligence and Elections," Mountain States Policy Center, February 6, 2024, https://www.mountainstatespolicy.org/the-good-and-the-bad-of-artificial-intelligence-and-elections.

163 Jackson et al., *Preparing for Artificial Intelligence and Other Challenges to Election Administration*.

164 Brittany Shepherd, "Americans' Faith in Election Integrity Drops: Poll," ABC News, January 6, 2022, https://abcnews.go.com/Politics/americans-faith-election-integrity-drops-poll/story?id=82069876.

165 Brennan Center for Justice, "Local Election Officials Survey"; and Norden et al., "States Take the Lead in Regulating AI in Elections."

166 Preparing Election Administrators for AI Act, S. 3897, 118th Cong. (2023–24), https://www.congress.gov/bill/118th-congress/senate-bill/3897/all-actions.

167 Akin Gump Strauss Hauer & Feld LLP, "Senate Rules Committee Reports Election-Related AI Bills Out of Committee," AI Law and Regulation Tracker, May 15, 2024, https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/Senate-Rules-Committee-Reports-Election-Related-AI-Bills-Out-of-Committee.

168 Exec. Order No. 14110, 88 Fed. Reg. 75191 (2023); and NIST, *Artificial Intelligence Risk Management Framework*.

169 DHS, "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure," November 14, 2024, https://www.dhs.gov/publication/roles-and-responsibilities-framework-artificial-intelligence-critical-infrastructure.

170 Owen J. Daniels and Jack Corrigan, "AI Won't Pause for the Election, and AI Regulation Shouldn't Either," FedScoop, September 27, 2024, https://fedscoop.com/ai-wont-pause-for-the-election-and-ai-regulation-shouldnt-either.

171 Alice Clapman and Andrew Garber, "A New Antidemocracy Tool," Brennan Center for Justice, September 5, 2023, https://www.brennancenter.org/our-work/analysis-opinion/new-antidemocracy-tool. See also Andrew B. Garber and cosignatories (counsel and nonprofit organizations), letter to Columbia County, GA, Board of Elections Chairperson Ann Cushman, members Wanda Duffie and Larry Wiggins, and Executive Director Nancy Gay re. EagleAI NETwork contract, October 16, 2023, https://www.brennancenter.org/sites/default/files/2023-10/Updated GA Letter EagleAI.pdf.

172 Robyn Sanders and Alice Clapman, "Protections Against Mass Challenges to Voter Eligibility," Brennan Center for Justice, July 17, 2024, https://www.brennancenter.org/our-work/research-reports/protections-against-mass-challenges-voter-eligibility.

173 Clapman and Garber, "New Antidemocracy Tool."

174 Alonzia Quinn and Helen Brewer, "Rules for Challenging Voter Eligibility Vary Across the States," National Conference of State Legislatures, September 27, 2024, https://www.ncsl.org/state-legislatures-news/details/rules-for-challenging-voter-eligibility-vary-across-the-states.

175 National Conference of State Legislatures, "Table 14: How States Verify Voted Absentee/Mail Ballots," October 9, 2024, https://www.ncsl.org/elections-and-campaigns/table-14-how-states-verify-voted-absentee-mail-ballots. See also Larry Buchanan and Alicia Parlapiano," Two of These Mail Ballot Signatures Are by the Same Person. Which Ones?," *The New York Times*, October 7, 2020, https://www.nytimes.com/interactive/2020/10/07/upshot/mail-voting-ballots-signature-matching.html.

176 CISA, "Signature Verification and Cure Process," accessed January 14, 2025, https://www.cisa.gov/sites/default/files/publications/signature-verification_cure_process_final_508.pdf.

177 Kyle Wiggers, "Automatic Signature Verification Software Threatens to Disenfranchise U.S. Voters," VentureBeat, October 25, 2020, https://venturebeat.com/ai/automatic-signature-verification-software-threatens-to-disenfranchise-u-s-voters; and Sarah M. L. Bender, "Algorithmic Elections," *Michigan Law Review* 121, no. 3 (December 2022): 489–522, https://michiganlawreview.org/journal/algorithmic-elections.

178 National Conference of State Legislatures, "Table 15: States with Signature Cure Processes," last updated January 6, 2025, https://www.ncsl.org/elections-and-campaigns/table-15-states-with-signature-cure-processes.

179 Brennan Center for Justice, AI and Elections Series, accessed January 14, 2025, https://www.brennancenter.org/series/ai-and-elections.

ABOUT THE AUTHORS

▶ **Mekela Panditharatne** is senior counsel in the Elections and Government Program, where her work focuses on election reform, election security, governance, voting, truth, and information. She has also guided initiatives related to technology and democracy. Panditharatne's writing has been published in *The New York Times*, *The Washington Post*, CNN, and NBC News. She has coauthored nationally recognized reports, and her writing has been entered into the Congressional Record.

▶ **Lawrence Norden** is vice president of the Elections and Government Program, where he supervises the Brennan Center's work in a variety of areas, including election infrastructure and security, election disinformation, and artificial intelligence. His work has been featured in media outlets across the country, including *The New York Times*, *The Wall Street Journal*, Fox News, CNN, MSNBC, and NPR. He is the lead author of the book *The Machinery of Democracy: Protecting Elections in an Electronic World* (Academy Chicago Press, 2006) and a contributor alongside his Brennan Center colleague Ian Vandewalker to *Defending Democracies: Combating Foreign Election Interference in a Digital Age* (Oxford University Press, 2021). He sat on the U.S. Election Assistance Commission's board of advisors from 2019 to 2023 and Aspen Digital's AI Elections Initiative Advisory Council in 2024.

▶ **Joanna Zdanys** is deputy director of the Elections and Government Program, focusing on advancing reforms in the areas of money in politics, election administration, artificial intelligence, and other democracy issues. Zdanys provides policy advice to lawmakers across the country, and her comments and work have been featured in media outlets including the *New York Times*, *Chicago Sun-Times*, *New York Law Journal*, and NBC. She is an adjunct professor of clinical law at NYU Law School, where she teaches a course on public policy advocacy. Zdanys holds a bachelor's degree in English from Yale College and a master's degree in English and comparative literature from Columbia University. She earned her JD from Fordham University, where she was the editor in chief of the *Fordham Urban Law Journal* and a Stein Scholar for the Public Interest.

▶ **Daniel I. Weiner** is director of the Elections and Government Program, where he leads the Brennan Center's work on money in politics, voting and elections, government ethics, and other democracy and rule of law issues. He has authored a number of nationally recognized reports and law review articles on election law and related topics. He also writes and comments regularly for media outlets such as *The New York Times*, *The Washington Post*, the *Los Angeles Times*, *The Wall Street Journal*, *Politico*, *Slate*, the *Daily Beast*, CNN, MSNBC, ABC News, and NPR. He has testified before Congress, state legislatures, and other governmental bodies, and he regularly provides legal and policy advice to leaders in Washington and across the country. Weiner received his JD from Harvard Law School.

▶ **Yasmin Abusaif** is counsel in the Elections and Government Program. Her work focuses on issues related to election administration, election security, and election disinformation. Before joining the Brennan Center, she worked as an associate in the Philadelphia office of Dechert LLP. She holds a BA from the College of William and Mary and a JD from the University of California, Los Angeles School of Law.

ACKNOWLEDGMENTS

The Brennan Center extends deep gratitude to all our supporters, who make this report and all our work possible. See them at brennancenter.org/supporters.

The authors are deeply grateful to their Brennan Center colleagues for their contributions. Abdiaziz Ahmed, Kathy Boockvar, Maya Kornberg, Gowri Ramachandran, and Derek Tisler contributed important insights and collaboration throughout. Shanze Hasan and Penelope Mack provided critical project management, research, and drafting assistance. Edgardo Cortes, David Evan Harris, Owen Doyle, and Liz Howard contributed essential insights and feedback. Faiza Patel, Amos Toh, and Emile Ayoub shared civil rights and civil liberties expertise. Former Parke Fellow Sophia Deng, legal intern Niyati Narang, and undergraduate intern Maya Adhikari provided research assistance. The communications expertise of Zach Laub, Marcelo Agudo, and Brian Palmer made the publication of this report possible. The authors also gratefully acknowledge the scholars and practitioners who generously shared expertise, knowledge, and feedback that informed this report: Jeremy Epstein (National Science Foundation), Ami Fields-Meyer (Harvard Kennedy School Ash Center for Democratic Governance and Innovation), Joshua Goldstein and Mia Hoffman (Georgetown's Center for Security and Emerging Technology), and Zeve Sanderson (New York University's Center for Social Media and Politics). Any mistakes are the authors' alone.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
brennancenter.org