

Student Working Paper Series

Generative Artificial Intelligence and the 2024 U.S. Election

How to regulate generative AI before 2024 U.S. Election?

Corbin Cerny, MPP 2025

Iana Lanceta, MPP 2025

Joshua Hyochan Lee, MPP 2024

Amritanshu Pattanaik, MPP 2025

16 April 2024

The threat of generative AI in the 2024 election necessitates swift action. Public concern underscores the seriousness of AI-driven misinformation, while real-world examples highlight the complexities of addressing this issue. Stakeholder analysis reveals a diverse landscape, emphasising the need for a multifaceted policy approach involving federal and state-level actors, as well as other key entities in the information ecosystem. Immediate state-level actions should focus on citizen engagement, digital literacy, and election worker support. Medium and long-term strategies must include criminalisation, moratoriums, disclosure requirements, private sector coordination, federal legislation, and revision of existing and outdated legal frameworks. These recommendations aim to fortify the American democratic process against unprecedented AI threats for 2024 and beyond.

#GenAI #USElection
#Misinformation

Table of Contents

1 Introduction	3
2 Policy Analysis	4
3 Stakeholder Analysis	8
3.1 The Federal Government	9
3.1.1 <i>Executive</i>	9
3.1.2 <i>Judicial</i>	9
3.1.3 <i>Congress</i>	10
3.2 National Political Parties (GOP and DNC)	10
3.2.1 <i>Republican Party (GOP)</i>	10
3.2.2 <i>Democratic National Committee (DNC)</i>	10
3.2.3 <i>Federal Agencies (FBI, DOJ, DHS, FEC):</i>	11
3.3 Social Media Platforms & Tech Companies	11
3.4 State Level Stakeholders	12
3.5 State Governments	12
3.6 Civil Society & Private Sector Stakeholders	14
3.6.1 <i>News Media Organisations</i>	14
3.6.2 <i>Civil Society Organisations</i>	14
3.6.3 <i>Think Tanks</i>	14
3.6.4 <i>Academic Institutions</i>	14
3.7 Interpreting the Stakeholder Map	15
4 Policy Instruments	15
4.1 Enforcement	15
4.2 Technology Integration	16
5 Policy Recommendations	16
5.1 Immediate Actions – State-Level Action Before the 5 November 2024 Election	17
5.2 Medium Term Action: State-Level Action Beyond 2024	18
5.3 Long Term Action: Federal and Private Sector Action	20
6 Conclusion	20
7 References	22

1 Introduction

Photographic manipulation is nothing new to the American electorate. Tampering with images of American political figures is nearly as old as photography itself. Civil War general and President Ulysses S. Grant's famous photo at City Point, Virginia, was doctored to show him on horseback among his troops. A composite of several photos, the image was likely created at the turn of the twentieth century (*Civil War Glass Negatives and Related Prints - Solving a Civil War Photograph Mystery*, 1861). At the start of this century, a picture of then President George W. Bush visiting with elementary school students was manipulated to show him reading a children's book upside down. The intent to portray Bush as unintelligent was another entry into the long list of political disinformation that has become a hallmark of American political campaigns (Jaffe, 2002).

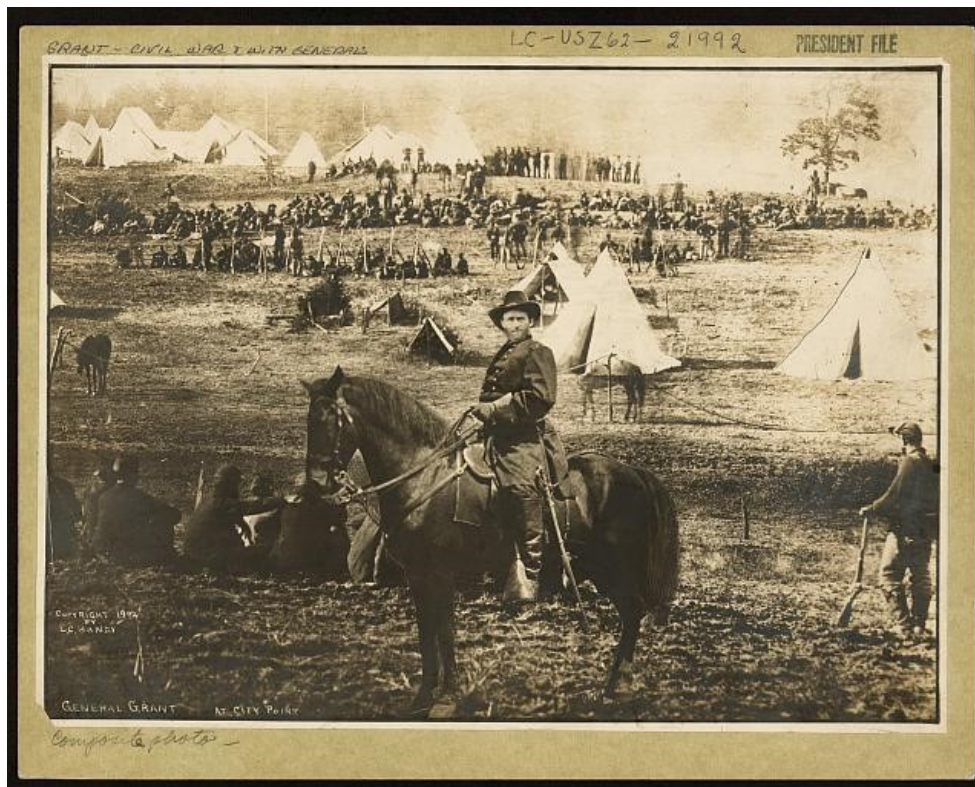


Figure 1 - This photo, titled "General Ulysses Grant at City Point" is a composite of three negatives created by Levin Corbin Handy in 1902.

Source: The Library of Congress of the United States of America, <https://www.loc.gov/> (2023)



Figure 2 - (right) Photograph of then President George W. Bush at George Sanchez Charter School in Houston, 2002; (left) Altered image showing Bush holding the children's book upside down.

Source: ResearchGate, <https://www.researchgate.net/> (2023)

The history of altered imagery in American politics is often seen as comical, with photos doctored into ridiculous and obviously false scenes or showing evident signs of alteration that are quickly exposed. However, technological advances of the last decade mean that future distortions risk being far more nefarious and damaging to the public information sphere.

Generative Artificial Intelligence (“generative AI”) is a technology that uses deep learning models and data training to generate hyper-realistic content that includes audio, images, and videos (Martineau, 2023). Given its technological sophistication, generative AI has created an unprecedented level of complexity to the issue of political misinformation. This increased complexity is particularly concerning in the American context since the dissemination of less sophisticated misinformation media before the 2016 election strongly affected voter choice in a partisan way (Allcott & Gentzkow, 2017). In preparation for the 2024 election, this paper provides cautionary case studies of generative AI misinformation and analyses the stakeholders and policy instruments. The culmination of this analysis is a set of medium and long-term strategies that centre on enforcement and technological integration frameworks.

2 Policy Analysis

Generative AI presents distinctive challenges to the American democratic process that have so far been unseen in previous election cycles. The new technology is widely accessible to the public, lowering barriers that previously made producing photographic, video, and audio disinformation out of reach for most people. The costs of software and other tools required for manipulating and producing content are not a factor for contemporary generative AI platforms. Likewise, new generative AI tools eliminate the skills necessary for users of graphics editors, like Adobe Photoshop, and can be accessed by anyone with an internet connection.

The quality of content produced by generative AI tools has drastically improved since the technology first became publicly accessible in the past decade, and quality continues to improve. AI models can learn from large amounts of data and

identify patterns that human users may not be able to see, resulting in more accurate and higher-quality content. Most photographic fakes produced by humans of our political past are simple edits that leave most of the source image intact with subtle changes to mislead the viewer. Human-altered content can also be crudely produced or outrageous in a subject that is clear, even at an initial glance, to be a distortion. By contrast, generative AI-produced content is far more complex and detailed – making it hard to detect by the layman – and higher quality deepfakes can take time for even professionals to debunk. In the time it takes to validate content as being AI-generated, it can spread widely and receive countless views.

Finally, generative AI makes disinformation scalable on an industrial level. The generative AI tools producing content can do so in seconds. Unique doctored material can enter the public information space at unprecedented rates. Generative AI's scalability, combined with its wide accessibility and rapidly improving quality, can potentially supercharge disinformation in the 2024 election cycle (Ryan-Mosley, 2023; Volpicelli, 2023).

The risk posed in the upcoming election is apparent to the American electorate. In August 2023, the AI Literacy Lab at Northeastern University in Nottingham surveyed 1,000 Americans aged 18+ to gauge the public feelings and attitudes concerning AI. Results showed that 83% worry about AI-driven misinformation and disinformation during the 2024 election cycle (How Americans See AI: Caution, Skepticism, and Hope, 2023).

How Americans See AI

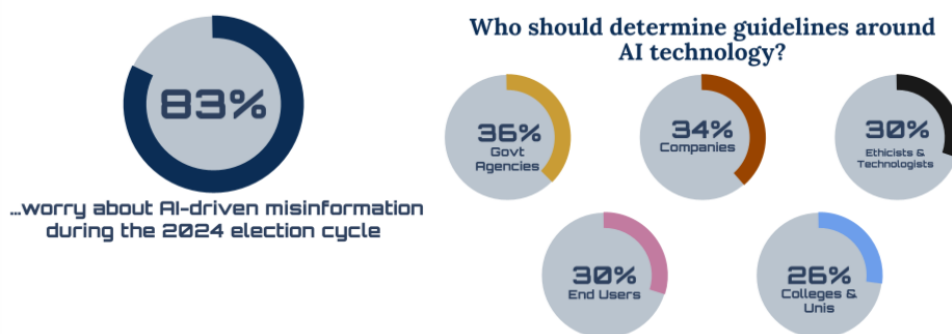


Figure 3 – The AI Literacy Lab's survey results on How Americas See AI (Skepticism, and Hope, 2023).

The risks posed to the election cycle are broadly defined by two categories: (1) the effect of AI-generated content to influence the electorate and (2) the erosion of the public's trust in the information space.

The first risk is straightforward – as fake content enters the public discourse, its impact could influence voters. The 2023 mayoral elections in Chicago is one of the first examples of AI-driven disinformation shared in an American

election. In the final days of the campaign, a video surfaced on the platform X (formerly known as Twitter) purporting to show the candidate Paul Vallas saying that “in my day”, a police officer could kill 17 or 18 people and “nobody would bat an eye” before going on to declare support for “refunding the police” (Hickey, 2023). The video was posted from a profile created only a few days before. The Vallas campaign reported the account, which was soon suspended, and published a press release denouncing the video as fake, but by that point, it had already been widely circulated.

Vallas was seen as the favourite to win the upcoming election, but he went on to lose by about 5 per cent. There is no way to say conclusively that the deepfake cost him the race, but realistic generative AI disinformation is, without a doubt, costly for candidates and misleading for voters. What happened in Chicago may be a precursor to the types of AI-generated disinformation that will appear in the 2024 election cycle.

The second risk is indirect, dealing with the impact of generative AI on the information space around elections – namely, the potential erosion of public trust in all media content. Wariness of fabrication makes the public more sceptical of accurate information, especially when a litany of fake content is circulating. Some politicians may profit from an informational environment saturated with disinformation. This side-effect is a result of what’s called the “liar’s dividend”. Daniella Citron and Robert Chesney, in their paper *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, argue that heightened public scepticism will make it easier for politicians to avoid accountability for truth (Citron & Chesney, 2019).

To meet the challenge of generative AI and disinformation more broadly, the federal government has taken some steps but has fallen short of what is needed. Some of the reasons for the failure are partisan divide in Congress, legal challenges of policies, slander campaigns and private sector indifference. Whatever the reason, these challenges are unlikely to dissipate in the near term.

The Department of Homeland Security’s (DHS) short-lived Disinformation Governance Advisory Board was set up in 2022 to advise DHS and the White House on efforts to identify false and misleading claims and share facts about security concerns, covering anything from elections to natural disasters. However, immediately after its formation, the board came under a disinformation assault. Its executive director resigned only two months after a barrage of disinformation defaming her character and credentials. Notably, attacks included AI-generated pornographic deepfakes. DHS

dissolved the board shortly after that, only four months after it was created (Panditharatne & Giansiracusa, 2023).

Disinformation campaigns employed by nonstate actors have proven effective at undermining federal attempts to counter disinformation and misinformation. Even within the American legal system, there has been pushback in the form of lawsuits against the federal government and the private sector. The case *Murthy v. Missouri*, pending before the Supreme Court, is the most prominent example. The suit, filed by multiple plaintiffs, accuses the federal government of utilising its agencies and influence over online platforms to censor conservative and conservative-leaning speech. The focus of the case pertains to efforts by both the Biden and Trump White Houses to mitigate the spread of misinformation, which involves coordination with tech companies and platforms like Twitter and Meta (*Murthy v. Missouri*, 2023).

The Supreme Court has lifted an injunction set by a lower court which prevented the federal government from contacting social media companies while the final verdict is pending. However, even with the injunction lifted, federal authorities and private companies may think twice before taking action to combat disinformation or risk additional lawsuits. Whether they emerge from online extremist sentiment or in courtrooms, these undercutting efforts have a chilling effect, dissuading further action to curb disinformation broadly and complicating any interest by the federal government and private sector to mitigate the disinformation threat posed by generative AI.¹

Congress has displayed some bipartisan legislative interest in regulating generative AI, but it is limited. The bipartisan *Protect Elections from Deceptive AI Act* was introduced in September 2023 and prohibited using AI-generated audio and visuals that are “materially deceptive” to influence elections or fundraise. However, while the consensus among lawmakers is welcoming, it is unlikely that any legislation would pass in time to impact the 2024 election. Additionally, as the election approaches, partisanship will rise, shrinking the appetite for bipartisan lawmaking (Levin & Downes, 2023).

While the federal government has had mixed success, state governments have passed legislation regarding the use of generative AI in elections in their jurisdictions. Texas led the nation in 2019, establishing criminal penalties for distributing deepfake videos created to influence election outcomes. California, Michigan, Minnesota, and Washington have followed Texas. Several other states are currently moving legislation. Notably, these

laws were passed with overwhelmingly bipartisan support, even in the partisan political climate, and they have often garnered unanimous approval when passing (Cappelletti & Swenson, 2023; Rozenshtein, 2023).

¹

ibid.

Key elements of these laws have included:

- ❖ Criminal penalties for violators.
- ❖ Coverage of multiple types of generative AI content, including video, imagery, and audio.
- ❖ Requirements to disclose when content is AI-generated. Crucially, many of these states require those disclosures to be evident visually to the viewer and not just encoded in the content script.
- ❖ Minnesota and California have included moratoriums on using all generative AI content, outlawing their distribution within a set timeframe before election day.

The laws passed at the state level are still largely untested legally. Questions regarding freedom of speech are inevitable, and challenges will likely increase. However, by narrowing the scope of the laws to cover activities around elections, states increase their chances in court. Additionally, as states vary their approaches to addressing the generative AI spectre, it provides a policy laboratory for developing practical approaches and examples for other states to emulate (Smith, 2023).

The interaction and tensions between different sources of authority over the issue are best seen by analysing the stakeholders more closely. Legal intricacies between executive, judicial, and legislative authorities, as well as the breakdown of state powers and the powers of private actors, create obstacles in the way of substantive policy solutions. Therefore, understanding the dynamic between state, federal, and private sector jurisdictions is integral in establishing policy strategies.

3 Stakeholder Analysis

A closer look at the actors involved in the policies around the 2024 U.S. election cycle reveals a complex array of stakeholders influencing electoral dynamics. At the federal level, the White House and its agencies establish crucial guidelines for addressing emerging generative AI risks in the short term. At the same time, Congress and the judiciary hold considerable sway

over implementing long-term policy solutions. Parallel to federal action, the influence exerted by states and private sector actors is significant and serves as a more accessible and deployable set of policy solutions. Navigating the policy stakeholder landscape necessitates a nuanced understanding of the actors involved, their interactions with one another, and the overlap in jurisdictions pertaining to policy design and implementation.

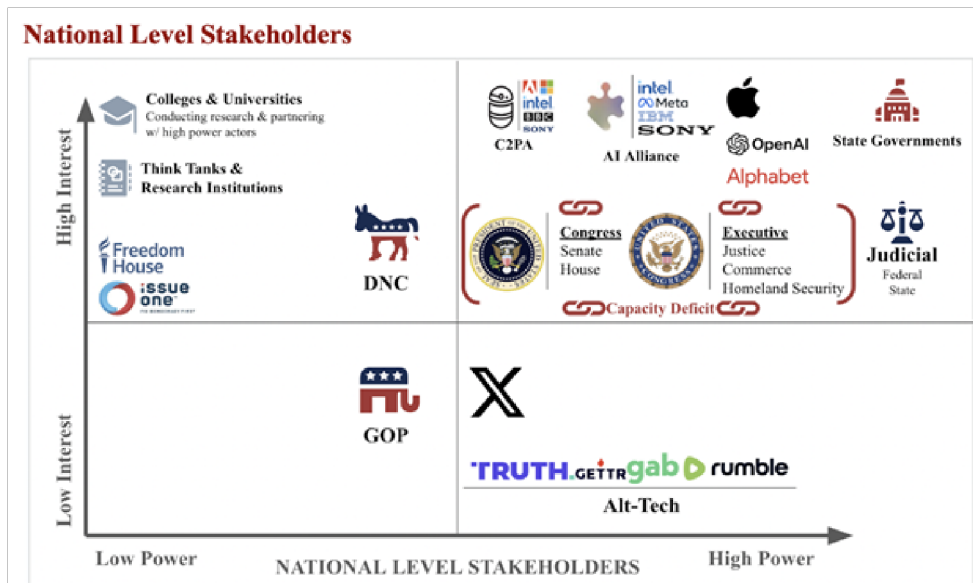


Figure 4 - Analysis of national level stakeholders in the generative AI debate (Image by Author).

3.1 The Federal Government

3.1.1 Executive

The administration's interest in generative AI spans national security, policymaking, public communication, international relations, and the appointment of key officials. Actions initiated within the executive branch wield significant influence over how the government navigates the challenges and opportunities posed by generative AI within electoral contexts. However, these actions are also obvious targets for individuals or groups aiming to thwart regulatory efforts.

3.1.2 Judicial

The judicial branch will scrutinise the application of any policy dealing with generative AI, particularly under the lens of freedom of speech and expression. There is little jurisprudence on the issue, leaving a large opening for the judiciary to interpret legal applications and set the parameters for future policies. However, there is no certainty on whether the judicial rulings will uphold policies aimed at reigning in the generative AI threat.

3.1.3 Congress

Bipartisan efforts will be instrumental in addressing the multifaceted challenges associated with AI technologies and elections. The members of Congress pictured below have displayed significant interest and hold positions capable of shaping policies.



Figure 5 - Congressional leaders demonstrating interest in AI regulation.

Source: Congress of the United States of America, <https://www.congress.gov/> (2023)

3.2 National Political Parties (GOP and DNC)

3.2.1 Republican Party (GOP)

Emphasising election integrity has been a critical theme for the GOP. However, during the 2024 election cycle, the GOP has deployed AI-generated deepfakes. In response to President Biden's re-election announcement, the GOP released an attack ad that used AI-generated content to showcase a second Biden administration in a dystopian fashion (Thompson, 2023). While Republican lawmakers may be interested in taking action, the party demonstrates a willingness to use technology to further its political agenda and influence voters (Thompson, 2023).

3.2.2 Democratic National Committee (DNC)

The DNC generally supports policies that address social justice, privacy, and inclusivity. In the context of generative AI, the party may advocate for regulations that prioritise these values while safeguarding the democratic

process. The ethical use of technology, particularly in elections, could be a key point. Focusing on ensuring that generative AI tools adhere to fairness, transparency, and accountability principles to protect voters' rights will likely be central to the DNC position.

3.2.3 Federal Agencies (FBI, DOJ, DHS, FEC):

Federal agencies, including the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), the Department of Homeland Security (DHS), and the Federal Elections Commission (FEC), have a collective interest in safeguarding the integrity of elections and addressing potential challenges posed by generative AI. Their roles encompass legal oversight, national security concerns, cybersecurity, investigation and prosecution, and regulatory guidance.

3.3 Social Media Platforms & Tech Companies

Social media and tech companies face content moderation challenges, especially when identifying and addressing AI-generated disinformation and deepfakes during the election cycle. Given the potential for AI-driven threats on their platforms, companies may enhance their security measures to protect against hacking, disinformation campaigns, and other risks that could compromise the integrity of the electoral process.

User education initiatives to enhance media literacy and critical thinking are a potential tool for companies seeking to educate their users on generative AI content risks. These initiatives could help users identify and resist manipulation attempts.

Social media companies may engage in policy advocacy and collaborate with policymakers to develop regulations and provide input on legislative initiatives to ensure alignment with industry practices. Collaboration could include releasing transparency reports detailing efforts to combat disinformation and providing insights into how they handle AI-generated content. Transparency promotes accountability and builds trust with users and policymakers.

Several companies have also spearheaded the creation of private sector coalitions, including other tech companies, academic institutions, and generative AI developers, with expressed interest in industry collaboration to regulate generative AI technologies and establish private sector-driven guardrails. The two most notable examples include the AI Alliance, which comprises Meta and IBM, and the Coalition for Content Provenance & Authenticity (C2PA), which includes Adobe, Intel, and Microsoft.

Not all social media and technology platforms share the same level of transparency, interest, and incentive regarding generative AI and its liability in the upcoming American. Certain companies have demonstrated a high interest in the responsible development and regulation of generative AI technology. They include Intel, Microsoft, SONY, Adobe, Meta, IBM, Open AI, Apple, Alphabet, and AI. Other companies, including X and right-wing platforms (known as alt-tech) such as Truth Social, Gab, Gettr, and Rumble, are driven primarily by ideological identity and have less interest in moderating generative AI use on their sites.

Social media and tech companies are crucial in shaping the information landscape. Their actions on generative AI, content moderation, user privacy, and collaboration with external stakeholders will significantly impact the integrity and fairness of the electoral process. Ideological sentiments jeopardise these efforts and create an environment where disinformation, including AI-generated content, can spread unchecked.

3.4 State Level Stakeholders

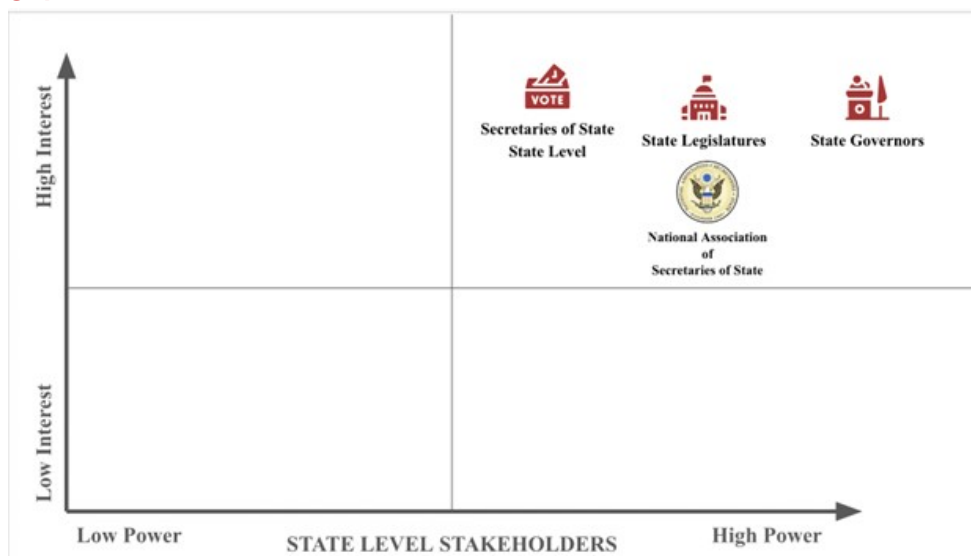


Figure 6 - State level stakeholders in the generative AI debate (Image by Author).

3.5 State Governments

State governments play a crucial role in elections and are important stakeholders with often unrecognised policy sway to regulate generative AI in the upcoming 2024 election.

- ❖ **Regulation and Oversight** – State governments have authority over elections within their jurisdiction. They may develop and implement

regulations and oversight mechanisms to address the use of generative AI in local and state-level electoral processes.

- ❖ **Compliance with State Laws** – State governments may ensure that the use of generative AI in elections complies with existing state laws. This could involve adapting current regulations or introducing new ones to address the unique challenges posed by advanced technologies.
- ❖ **Election Security** – Ensuring the security of elections is a primary responsibility of state governments. This includes assessing how generative AI technologies impact election security and taking measures to safeguard against potential threats, fraud, or manipulation.
- ❖ **Technology Infrastructure** – Some state governments, including Colorado, Utah, Georgia, and South Dakota, have invested in and upgraded their technology infrastructure to accommodate generative AI tools responsibly (Wood, 2023). Other states, such as California, are following suit and preparing to incorporate generative AI tools (*Governor Newsom Signs Executive Order to Prepare California for the Progress of Artificial Intelligence*, 2023). The adoption by states thus far includes generative AI use for data storage, cybersecurity, and integration into management frameworks.
- ❖ **Collaboration with Federal Agencies** – State governments often collaborate with federal agencies involved in election oversight, like the Federal Election Commission (FEC, responsible for enforcing campaign finance law), the Election Assistance Commission (a national clearinghouse and resource of information regarding election administration), and the Cybersecurity and Infrastructure Security Agency (an agency within the Department of Homeland Security charged with protecting the nation’s critical infrastructure, including election systems). They may work with agencies like the FEC to establish guidelines and protocols for using generative AI in elections.
- ❖ **Public Awareness and Education** – State governments may engage in public awareness campaigns to educate voters and election officials about the role of generative AI technology. This includes transparency about how these technologies can be used and their potential impact on election outcomes.
- ❖ **Private Sector Influence and Regulation** – Certain states hold outsized sway over the generative AI industry and connected sectors thanks to varying factors. Notably, California, Texas, and

Washington have considerable leverage due to many leading tech companies in their states. States can use this power and network to influence private sector policy on generative AI.

- ❖ **Secretaries of State** – The office of the Secretary of State is vested with overseeing, implementing, and securing elections. These offices establish policy and set deadlines, guidelines, and other important requirements for political campaigns to meet to get placed on the ballot. The custodianship of elections is an important tool for states to utilise when determining how to enforce measures regulating generative AI.

3.6 Civil Society & Private Sector Stakeholders

3.6.1 News Media Organisations

News organisations serve as primary conduits for disseminating information to the public. Despite their varying political positions, all news organisations share a multifaceted role in addressing the challenges and opportunities presented by generative AI. Their commitment to ethical journalism, fact-checking, public education, and adaptation to new technologies is essential for maintaining the integrity of the information ecosystem during election.

3.6.2 Civil Society Organisations

Civil Society Organisations (CSOs) serve as critical advocates for democratic values, ethical AI use, and the protection of civil liberties in the face of emerging technologies like generative AI. Their efforts contribute to a robust and inclusive discussion on the role of AI in election, ensuring that the interests of the broader public are represented and protected. Two notable CSOs influencing the debate on generative AI across different states are Issue One and the Brennan Center for Justice.

3.6.3 Think Tanks

Through research, analysis, collaboration with policymakers, and educational initiatives, think tanks contribute valuable expertise for regulating AI technologies in the national electoral process. Some leading think tanks on generative AI include Freedom House, Chatham House, and The Council on Foreign Relations (CFR).

3.6.4 Academic Institutions

Academic institutions play a central role in generating knowledge, fostering education, and contributing to the ethical and responsible use of generative AI. Their research and engagement activities help address challenges, inform policies, and shape the trajectory of AI in the electoral landscape.

Many of these institutions produce essential research informing policymakers in public and private spaces. Academic institutions are participating in the AI Alliance and the C2PA coalition, advising private sector actors.

3.7 Interpreting the Stakeholder Map

The convergence of generative AI and the 2024 U.S. election cycle underscores the critical need for strategic policy interventions. Understanding the multifaceted involvement of federal government actors, political parties, tech companies, state governments, and other groups is pivotal for crafting responsive solutions. Crucially, by analysing the involved actors, the policy instruments at their disposal are made evident, as are the points where their instruments may clash.

4 Policy Instruments

The capacities of these stakeholders provide the basis for selecting policy instruments. The stark divisions that shroud the elections necessitate careful selection of policies, navigating the ever-shrinking bipartisan space in American politics. Safeguarding elections remains a unifying call for the American public. Determining how to go about this, however, reveals the growing fissures. Creative policy instruments that address institutional knowledge gaps, oversight, and targeted enforcement mechanisms offer rare policy overlap between factions. These methods are explored closely, given the rampant partisanship surrounding policy actors and the technological sophistication of the issue.

4.1 Enforcement

While regulation seeks to achieve objectives that would not be obtained otherwise, enforcement compels parties to do (or not do) certain things and is, therefore, central to regulation compliance. The contentiousness between the need to contain the dissemination of political misinformation and the value placed on freedom of speech necessitates using enforcement as a critical policy instrument. Rule design (i.e., legal language) can clarify the differences between freedom of speech and misinformation violations. At the same time, enforcement tactics will allow policymakers to deter parties from creating AI-generated misinformation and establish consequences for those who do.

Enforcement can go beyond rule design and punishment by inadvertently instigating positive behavioural change to maximise the strategic value of

enforcement measures. It is essential to have the following questions guide enforcement design:

- ❖ What are the motivations behind specific behaviour?
- ❖ What are appropriate reactions to non-compliance?
- ❖ Who should be responsible for enforcement?

4.2 Technology Integration

A technology-oriented approach involves technological prescriptions to underpin policy design. On the one hand, technological integration can present many advantages to homogenous organisations that can expect consistency in the benefits of a particular technological prescription. Such advantages can include improved efficiency and opportunities for process automation in problem detection. Moreover, it can promote evidenced-based strategy development by enabling organisations and policymakers to identify trends in the data reported from the technological prescription. The importance of such data can be seen in quickly detecting the origins of AI-generated misinformation. However, technology-driven policies have some limitations, such as not being effectively applicable to a heterogeneous group of actors. This means a uniform technological prescription cannot be imposed on large and small organisations in different sectors because these actors' capacities and central concerns are varied. Thus, technological integration policies should be approached in a way that targets specific organisations within industries to maximise their benefits.

The instruments discussed provide the theoretical framework for policy recommendations. However, implementing the policies and programs requires further strategic planning and discussion, considering the fast-approaching election timelines, long-term goals regarding misinformation prevention, and suitability among state and federal actors.

5 Policy Recommendations

As the 2024 election looms, immediate and short-term actions at the state level are imperative. Federal and state governments and federal state agencies must undertake medium and long-term strategies to establish comprehensive guardrails against generative AI-produced disinformation.

5.1 Immediate Actions – State-Level Action Before the 5 November 2024 Election

With the 5 November 2024 election less than a year away at the time of publication, the viability of state-level legislative action is diminished. The implementation timeline for legislation exceeds a year in every state, and the use of emergency powers to expedite implementation is unrealistic at the level needed to have any significant impact. States should focus instead on initiatives that are possible outside of the legislative process regarding safeguarding the 2024 election cycle.

- ❖ **Engage with grassroots citizen efforts to identify and flag disinformation** – Grassroots organisations and actors have proven effective at flagging fake content online. A practical example of coordination between grassroots initiatives and state authorities can be seen in Lithuania, where a coalition of citizen fact-checkers known as “elves” and the Lithuanian Ministry of Defence have coordinated to fight Russian disinformation (Abend, 2022). This approach has made the country a leader in counter-disinformation strategy, and it should be investigated for implementation by states.
 - **A reporting portal** through the state election office would be established that allows citizen reporting of disinformation to election officials.
 - **Soft organisation** of active citizen groups interested in identifying disinformation. University and college student groups could provide a source of passionate and skilled “elves” who are already loosely organised and can be mobilised quickly.
- ❖ **Civil education initiatives and digital literacy training** – States should invest in resources and initiatives to train and educate their electorate to identify and report AI-generated disinformation. While generative AI outputs are improving quickly, it is still possible to identify false content. Evidence that content is synthetically produced is visible, and there are tools available to the public that can help.
 - **A media campaign** through television, radio, online, and printed press to disseminate knowledge and provide access to resources for voters.

- **Workshops** held at community centres, libraries, and other accessible and politically neutral venues covering digital literacy.
- ❖ **Support and training for election workers** – As was the case in 2020, volunteers at polling stations in 2024 will be critical players in debunking disinformation surrounding the election and targets of those disinformation efforts. State election offices must train these volunteers on generative AI content and provide security and wellbeing resources.
- ❖ **Formation of state advisory boards** – In preparation for legislative action and to advise on the current election cycle, states should form advisory boards of policymakers, civil leaders, and other vital actors to begin framing the necessary policies to follow in 2024. The sooner this work can begin, the sooner policies can be implemented.

5.2 Medium Term Action: State-Level Action Beyond 2024

While state-level legislation is unlikely to affect the landscape before November 2024, states must begin now to move legislation forward in preparation for future elections. Legislation has already been tried and proven in several states, providing a template for others to replicate and expand upon.

- ❖ **Criminalisation of certain political uses of generative AI** – The use of generative AI in the political environment is inevitable. Improper use of the technology should be clearly defined within the context of election and punished accordingly.
 - **Attacking election/poll workers and volunteers** has increased since the 2020 election. They are particularly vulnerable to generative AI deepfakes and other disinformation. Therefore, laws that strictly outlaw and penalise using technology to harass these individuals and their relatives must be adopted.
 - **Attacking candidates and their families** in certain ways should be penalised. While it is unlikely to restrict all use of the technology to attack candidates, certain tactics must be criminalised. This can include using deepfake technology to attack candidates' families or staff and its use to create pornographic and disproportionately false content of the candidate.
 - **Suppressing voters from certain groups** is a common tactic by bad actors in elections, and generative AI technology

could increase the frequency and effectiveness of their attacks. For example, generative AI could be used to send misleading phone calls to a targeted segment of the population (Chung, 2022). The use of technology to suppress voters in this way and in other ways must be penalised.

- ❖ **Moratorium on AI-generated content before an election** –As witnessed in the 2023 Chicago Mayoral Election and the Slovakian Parliamentary Elections, disseminating generative AI content close to an election day can amplify its effects and make it challenging to debunk. While it is impossible to prevent these instances, state legislatures should adopt moratoriums in the lead-up to election days where it is illegal to disseminate any content created through generative-AI, as has been done in California and Minnesota.
- ❖ **Disclosure requirements that are clearly visible to content consumers** – Clear and defined generative AI content disclosures should be adopted by states for campaigns, candidates, and other political actors to disseminate and circulate any content generated by AI. Generative AI producers and distributors should also be required to include disclaimers on their products, but not as an alternative to the candidates themselves or their campaigns and associated PACs. Disclaimers, in addition to being embedded in the content coding, should also be readily ascertained by voters. Image and video content should visibly display a disclaimer evident to viewers, and audio deepfakes should include aural disclaimers for listeners.
- ❖ **Formalisation of coordination avenues with the private sector** – Certain states (such as California, Washington, Texas, and New York) possess disproportionate influence over the tech sector, including social media, search engines, streaming platforms, and generative AI content producers. These states should use their leverage to coordinate with and lobby on behalf of all states for action from private sector actors.
 - **The AI Alliance and the Coalition for Content Provenance & Authenticity (C2PA)** have the tech industry’s leading companies among their members, many of which are headquartered in the same handful of states above. These states should actively participate with these two collectives, if not seek active membership to shape and influence private sector actions.
 - **Coordination among the states will be crucial**, especially as some states hold disproportionate sway compared to others.

State governments should coordinate their efforts, especially as it relates to engagement with the private sector.

- **A summit of secretaries of state and of governors** should be organised to instigate inter-state coordination and demonstrate the organised interest of state authorities in regulating the political use of generative AI.

5.3 Long Term Action: Federal and Private Sector Action

Though states can take short-term action independently, federal action and national legislation are necessary to adequately address the generative AI spectre on elections beyond 2024. State-level action is effective immediately when federal action is unlikely, but it is a patchwork approach that can only address the symptoms of the more significant issue. To comprehensively address threats from the inevitable use of generative AI content, the federal government must establish a national approach that fills in the policy gaps that states cannot cover.

Federal legislation is crucial to standardise the legal framework for generative AI in elections. Bipartisan support for legislation preventing deceptive AI use in elections is promising. It is imperative to defend and adapt these laws against judicial scrutiny. Regulation of the private sector is vital, necessitating national mandates and penalties for clear AI disclaimers. While states can regulate within their jurisdictions, a national approach ensures compliance and imposes federal legal action. Addressing foreign-origin generative AI disinformation, especially from foreign actors, demands a nationwide strategy. Revisions to Section 230 are necessary, mandating thresholds for social media and generative AI companies. This step ensures platform security, transparency, and information sharing, with bipartisan support evident.

6 Conclusion

Generative AI technology is advancing at a rapid and increasing pace. As a result, its presence and use in society and politics are unavoidable. American state and federal authorities, as well as the private sector, must act with urgency now to avoid falling too far behind the technology's development. The best path forward is to embrace generative AI as inevitable in our domestic politics and establish guardrails that treat it as such. Allowing generative AI to develop unchecked and to impact our electoral processes without considering and preparing for the impact would be catastrophic for the health of democracy. By leading initially from the state level and legislating up to the federal level, the United States can safeguard the fast-

approaching 2024 elections while preparing for the generative AI influence in subsequent elections.

7 References

Abend, A. (2022, March 5). *Meet the Lithuanian 'Elves' Fighting Russian Disinformation.*

TIME. <https://time.com/6155060/lithuania-russia-fightingdisinformation-ukraine/>

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election.

Journal of Economic Perspectives, 31(2), 211–236.

Cappelletti, J., & Swenson, A. (2023, November 29). *Michigan to join state-level effort*

to regulate AI political ads as federal legislation is pending. PBS NewsHour.

<https://www.pbs.org/newshour/politics/michigan-to-join-state-level-effortto-regulate-ai-political-ads-as-federal-legislation-is-pending>

Chung, C. (2022, December 1). They Used Robocalls to Suppress Black Votes. Now

They Have to Register Voters. *The New York Times.*

<https://www.nytimes.com/2022/12/01/us/politics/wohl-burkman-votersuppression-ohio.html>

Citron, D., & Chesney, R. (2019). Deep Fakes: A Looming Challenge for Privacy,

Democracy, and National Security. *California Law Review*, 107(6), 1753.

Civil War Glass Negatives and Related Prints—Solving a Civil War Photograph Mystery.

(1861). The Library of Congress.

<https://www.loc.gov/pictures/collection/cwp/mystery.html>

Governor Newsom Signs Executive Order to Prepare California for the Progress of

Artificial Intelligence. (2023, September 6). Office of Governor of California.

<https://www.gov.ca.gov/2023/09/06/governor-newsom-signs-executiveorder-to-prepare-california-for-the-progress-of-artificial-intelligence/>

Hickey, M. (2023, February 27). *Vallas campaign condemns deepfake video posted to*

Twitter. CBS Chicago.


<https://www.cbsnews.com/chicago/news/vallascampaign-deepfake-video/>

- How Americans see AI: Caution, skepticism, and hope.* (2023). [Survey]. AI Literacy Lab Northeastern University. <https://ai-literacy.northeastern.edu/poll-howamericans-see-ai-caution-skepticism-and-hope/>
- Jaffe, J. (2002, November 16). *Dubya, Willy Turn the Book Over?* *Wired*. <https://www.wired.com/2002/11/dubya-willya-turn-the-book-over/>
- Levin, B., & Downes, L. (2023, May 19). *Who Is Going to Regulate AI?* *Harvard Business Review*. <https://hbr.org/2023/05/who-is-going-to-regulate-ai>
- Martineau, K. (2023, April 20). *What is generative AI?* | *IBM Research Blog*. IBM Research Blog. <https://research.ibm.com/blog/what-is-generative-AI>
- Panditharatne, M., & Giansiracusa, N. (2023). *How AI Puts Elections at Risk—And the Needed Safeguards*. Brennan Center for Justice. <https://www.brennancenter.org/our-work/analysis-opinion/how-ai-putselections-risk-and-needed-safeguards>
- Rozenshtein, A. (2023, May 24). *Prof. Alan Rozenshtein Interviewed by Minnesota Lawyer on MN Legislation to Regulate Deepfakes* [Interview]. <https://law.umn.edu/news/2023-05-24-prof-alan-rozenshtein-interviewedminnesota-lawyer-mn-legislation-regulate>
- Ryan-Mosley, T. (2023, October 4). *How generative AI is boosting the spread of disinformation and propaganda.* *MIT Technology Review*. <https://www.technologyreview.com/2023/10/04/1080801/generative-aiboosting-disinformation-and-propaganda-freedom-house/>
- Smith, C. (2023, October 27). *States Act, but Can Legislation Slow AI-Generated Election Disinformation?* *Governing*. <https://www.governing.com/policy/states-act-but-can-legislation-slow-ai-generated-election-disinformation>

Thompson, A. (2023, April 25). *Republicans slam Biden re-election bid in AI-generated ad*. Axios. <https://www.axios.com/2023/04/25/rnc-slams-biden-re-electionbid-ai-generated-ad>

Volpicelli, G. (2023, October 23). *AI and the end of photographic truth*. POLITICO. <https://www.politico.eu/article/ai-photography-machine-learningtechnology-disinformation-midjourney-dall-e3-stable-diffusion/>

Wood, C. (2023, October 11). *State CIOs share early use cases for generative AI*. StateScoop. <https://statescoop.com/state-government-generative-ai-uses/>



Alexanderstr. 3
D – 10178 Berlin
Tel.: +49 (0)30 259219 -0

Online: hertie-school.org/centre-for-digital-governance/
E-mail: digitalgovernance@hertie-school.org
LinkedIn: [linkedin.com/school/centre-for-digital-governance](https://www.linkedin.com/school/centre-for-digital-governance)

This publication reflects only the personal views of the authors. Publication under Creative Commons license CC BY-ND. Reprinting and other distribution – including excerpts – permitted only with acknowledgment of source • original version © Centre for Digital Governance – Hertie School, Berlin 2024