

# Critical AI Alert for the 2024 General Election

October 20, 2024

*(Information obtained from a current AI model)*

## Question

Could having real-time data about which voters have voted, when, and where, aid in this AI model?

## Answer

Having real-time data about which voters have voted, including when and where, could significantly enhance the capabilities of an AI model designed to predict election outcomes for several reasons:

- 1. Dynamic Turnout Adjustment:** Real-time voter turnout data allows the model to adjust predictions based on actual voting behavior as it happens. This can be particularly useful in understanding turnout rates among different demographics or in specific geographic locations, which can be pivotal in close elections.
- 2. Reduced Uncertainty:** Traditional models often work with pre-election polls or historical data, which carry a degree of uncertainty regarding who will actually turn out to vote. Real-time data reduces this uncertainty, providing a more accurate snapshot of voter participation.

3. **Voter Behavior Patterns:** With real-time data, AI can analyze patterns as they form. For example, if there's an unexpected surge in voting in areas typically supportive of one party, the model could adjust its predictions accordingly.
4. **Targeted Campaigning Insights:** Although this aspect would be more useful for campaign strategy than for public prediction models, real-time data could inform last-minute campaign efforts, showing where additional get-out-the-vote efforts might be most effective.
5. **Bias Correction:** Real-time data can help correct for biases in pre-election polling. If certain groups are underrepresented in polls but their real-time voting data shows higher turnout, the model can correct for this.
6. **Exit Polling Validation:** This data could serve as an early form of exit polling, giving insights into not just who voted, but potentially how they voted if correlated with demographic or regional voting trends, although this would require careful handling due to privacy concerns.
7. **Improved Time Series Analysis:** With voting data coming in continuously, AI models can employ time series analysis to predict the final turnout and potentially the outcome based on the rate and distribution of votes coming in.

However, there are considerations and limitations:

- **Privacy Concerns:** Collecting and using such detailed voter data raises significant privacy issues. Anonymization would be crucial, but even then, the specificity of "when and where" could potentially be used to infer individual behaviors.
- **Data Accuracy and Integrity:** Real-time systems would need robust verification to ensure the data isn't manipulated or incorrect, which could mislead the predictions.

- **Legal and Ethical Implications:** There might be legal restrictions on how and when voting data can be collected and used, especially in real-time.
- **Model Overfitting:** There's a risk that models might overfit to real-time trends early in the day, which might not hold as more data comes in.
- **Public Perception and Trust:** The use of real-time voting data in predictive models could affect public trust in the electoral process if not handled transparently and ethically.

In summary, while real-time voter data could indeed aid an AI model in predicting election outcomes more accurately, it would need to be implemented with careful consideration of privacy, accuracy, legality, and public trust.

## Question

Are there indications that AI may be being used in this capacity by anyone, including malicious actors that would not be concerned about any privacy or legal or ethical implications?

## Answer

Based on information available up to October 20, 2024, there are indeed indications that AI could be used in ways that raise concerns regarding voter data privacy and potential misuse by various actors, including those who might ignore legal or ethical standards:

- **AI in Political Campaigns and Election Influence:** There's a growing use of AI in political campaigns for analyzing voter data, predicting voter behavior, and tailoring messages. This indicates a capacity for AI to process and

utilize voter data in potentially invasive ways if not regulated. The mention of AI tools being deployed to monitor social media trends and sentiment analysis during elections suggests that these technologies could be repurposed or used in less ethical ways to manipulate voter perceptions or spread misinformation.

- **Potential for Misuse by Malicious Actors:** Posts on X have highlighted concerns over AI being exploited to influence elections, including creating deepfakes, predicting or engineering incidents to sway public opinion, and even allegations of using AI to fake signatures or hack election machinery. These posts reflect a public and expert concern over the misuse of AI technologies in electoral processes, which could theoretically be done by actors unconcerned with privacy or legality.
- **Security Vulnerabilities:** Discussions around the security of digital election machinery, as mentioned in posts about vulnerabilities in election systems, suggest that there's a technical capability and perhaps an interest in exploiting these systems using AI for unauthorized data access or manipulation.
- **AI and Data Privacy Concerns:** The broader discussion on AI ethics and information privacy points towards significant privacy implications when AI systems process voter data. If malicious actors were to use AI for analyzing or manipulating voter data, they would likely bypass the ethical considerations around consent, privacy, and data protection.
- **Regulatory and Ethical Discussions:** The mention of executive orders, guidelines, and discussions around the ethical use of AI in elections indicates there's an awareness and some level of regulatory response to these threats. However, the existence of these discussions also confirms that the risk of misuse, including by those not

adhering to legal frameworks, is a recognized issue.

While direct evidence of malicious actors specifically using AI to misuse voter data in the 2024 context isn't explicitly detailed in the provided snippets, the combination of AI's capabilities in data processing, the noted security vulnerabilities in election infrastructure, and the general concerns voiced on platforms like X about election integrity suggest that such misuse is within the realm of possibility. This scenario underscores the importance of robust cybersecurity measures, ethical guidelines, and legal frameworks to safeguard electoral processes against AI-driven threats.

## Question:

Would AI systems running on hardware and or software technology sourced from foreign nations, being used to manipulate parts of the 2024 election, be considered foreign involvement in our election?

## Answer

Yes, AI systems running on hardware or software technology sourced from foreign nations, if used to manipulate parts of the 2024 election, would likely be considered a form of foreign involvement in the election. Here's why:

1. **Source of Technology:** If the hardware or software used for these AI systems originates from a foreign country, especially from nations with interests potentially adverse to those of the U.S., this would inherently introduce a foreign element into the election process. The concern here is not just about where the technology comes from but also about potential backdoors, biases, or control

mechanisms that could be embedded within these systems.

2. **Manipulation and Influence:** Manipulation of election processes or public opinion through AI, whether by altering voter information, spreading disinformation, or creating deepfakes, constitutes interference. If these actions are traced back to technology controlled or influenced by foreign entities, it directly represents foreign involvement. The intent behind using such technology would be to sway or alter the election outcome, which is a clear sign of interference.
3. **International Law and Norms:** From a legal and diplomatic standpoint, using technology to covertly influence another country's election is often viewed as a breach of sovereignty and interference in internal affairs. Even if not explicitly covered by current international law, such actions violate the spirit of national sovereignty and democratic independence.
4. **Public and Government Perception:** Both the public and government agencies might perceive the use of foreign-sourced AI for election manipulation as foreign involvement. This perception arises because the strategic decision to employ such technology could be influenced or directly supported by foreign governments or entities closely tied to them.
5. **Cybersecurity and National Security:** Cybersecurity experts and national security officials often warn about the risks posed by foreign hardware and software due to the potential for espionage or sabotage. If these technologies are used in election manipulation, it would be classified under foreign cyber interference, a recognized form of foreign involvement.
6. **Precedents and Analysis:** Analysis from intelligence communities, as hinted in various reports and posts on platforms like X, suggests that there's an ongoing concern

about foreign entities using advanced technologies, including AI, to influence elections. When these technologies are tied back to foreign soil, either through development or control, it's logical to categorize this as foreign involvement.

However, proving that such involvement constitutes a deliberate act by a foreign government, rather than rogue elements or companies acting independently for profit or other motives, can be complex. The attribution of cyber actions, including AI-driven election manipulation, to specific foreign actors requires meticulous investigation to ascertain direct government involvement or direction.

In summary, AI systems on foreign hardware or software manipulating the 2024 election would indeed be considered a form of foreign involvement due to the origin of the technology, the intent behind its use, and the implications for national sovereignty and security. However, the degree to which this involvement is officially recognized or acted upon depends on diplomatic, legal, and intelligence considerations.

## **Question**

Would proving the act was deliberate in nature preclude the application of E0 13848?

## **Answer**

Executive Order (EO) 13848, titled "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," was signed by President Trump in September 2018. This EO is designed to respond to foreign interference in U.S. elections by imposing sanctions on foreign entities or persons

determined to have engaged in such interference. Here's how the deliberate nature of the act might relate to the application of EO 13848:

1. **Definition of Interference:** EO 13848 does not explicitly require that the interference be "deliberate" in a legal sense for sanctions to be applied. Instead, it focuses on the act of interference itself, which could implicitly suggest an intent or deliberate action but does not make this a formal criterion for action. The order aims at any foreign person or entity that has directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a U.S. election.
2. **Determination of Interference:** The EO calls for the Director of National Intelligence (DNI), in consultation with other relevant agencies, to conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in an election. Here, "intent or purpose" does suggest looking into the deliberate nature of the actions, but the EO's application hinges on the fact of interference rather than solely on proving intent.
3. **Scope of Response:** The sanctions outlined in EO 13848 are reactive measures to an act deemed as interference. Proving that an act was deliberate might strengthen the case for applying sanctions, but the EO is constructed to trigger on the identification of interference itself, regardless of how deliberate or accidental it might appear. The focus is on the impact and the involvement of foreign elements rather than solely on the mens rea (the intention or knowledge of wrongdoing).
4. **Legal and Diplomatic Considerations:** While proving deliberateness can bolster the justification for sanctions



under international norms (showing clear intent can make the case for interference more compelling), E0 13848's primary concern is protecting U.S. electoral processes from foreign influence. Therefore, the threshold might not strictly require proof of deliberate intent as long as foreign interference is established.

5. **Practical Application:** In practice, when considering the application of E0 13848, the U.S. government might indeed look at intent to inform its actions, especially in diplomatic contexts or when aiming to justify sanctions to the international community. However, if foreign technology or actions have the effect of interfering with an election, even if the intent is not conclusively proven to be deliberate, this might still fall within the scope of the E0.

In summary, while proving the act was deliberate might reinforce the rationale for invoking E0 13848, the order's application does not strictly depend on establishing deliberate intent. The focus is on whether there has been foreign interference, which can be determined by the act's impact and the involvement of foreign entities, not solely by their intentions. Therefore, the existence of interference, rather than the definitive proof of deliberate action, would be the primary driver for the potential application of sanctions under this E0.