HYPERLOCAL VOTER SUPPRESSION

AN A.I. ELECTION RISK CHECKLIST

BY: ASPEN DIGITAL'S
A.I. ELECTIONS ADVISORY COUNCIL

People may decide not to vote if they are confused about voting rules or concerned about conditions at voting sites. Historically, false information has been used to discourage voting within specific geographic areas or among particular identity-based communities.

AI tools can be used to create highly personalized and interactive content that misleads people about conditions at voting sites, voting rules, or whether voting is worthwhile.

MISUSE EXAMPLES

- Targeted text messages claim long lines at specific voting sites (e.g., *Voters are waiting six hours at Peace Elementary).*
- Fake local news website spreads false information about voting rules (e.g., *Charlotte Tribune: You'll need two IDs on Election Day*).
- Interactive robocalls alert people of road closures in a named area on Election Day.
- Fake images depict protests or violence in a specific city on Election Day.

MITIGATIONS

NEWS MEDIA, ADVOCATES, AND CIVIL SOCIETY

- Inform voters they may be targeted with false content that is highly specific or personal.
- Help voters understand false content may come to them in texts, messaging apps, and phone calls.
- Encourage voters to act only on election information from official sources and trusted news, and guide people to those sources.
- Underscore that intentional misrepresentations of voting rules is a felony [CRS].
- Establish relationships with election officials and cultivate authoritative sources on elections.

Interested in learning about other AI election risks? Visit www.aspendigital.org/ai-election-risks for more risk checklists.

ELECTION ADMINISTRATORS

- Proactively message voting rules (e.g., ID requirements, changes in polling hours, new polling locations) and promote early voting options.
- Use *.gov* website domains and seek verification (checkmarks/badges) across social media and messaging channels. Include a *.gov* link in any text messages sent to voters.
- Develop a rapid-response communication plan that alerts local news, key community leaders, and the public to counter false claims.
- Ensure agency websites and social media can be updated quickly in a crisis.
- Monitor social media throughout the election period and communicate with social media platforms, where appropriate.
- Partner with trusted messengers (e.g., leaders in the business, faith, veterans, or language-minority communities) to promote official election information and to encourage voters who see misinformation or have questions to reach out to election offices.

SOCIAL MEDIA

- Elevate reliable sources of election information in content feeds.
- Establish dedicated channels across major social media platforms for election officials and trusted partners to flag false claims about voting rules and voting sites.
- Review existing integrity tools in the context of AI-enabled variation (e.g., assumptions around virality prediction classifiers). Hyperlocal content may not trigger virality metrics. Review crisis protocols across surfaces.
- Use AI tools to monitor content-level narratives to identify trends and detect malign influence actors that may vary language to avoid detection.
- Proactively monitor content for civic policy violations (e.g., proactive sweeps across content originating in or discussing sensitive election jurisdictions).

MESSAGING APPS & SERVICES

- Adopt content rules that explicitly prohibit local voter suppression.
- Notify users that false messages about elections logistics may appear, and encourage users to report such messages and to verify claims regarding voting rules and voting sites via official sources.
- Review integrity monitoring of open one-to-many messaging features, especially those focused on a particular geography or demographic identity.
- Consider posting rate limits and restrictions on new accounts.

A.I. LABS, DEVELOPERS, & COMPANIES

- Adopt usage policies prohibiting local voter suppression.
- Respond to voting queries by directing users to official sources using a hyperlink and noting that it is important to verify voting information with official sources.
- Review integrity detection and tooling (e.g., to detect spikes in model completions/outputs about voting rules or voting sites or in requests to generate a high number of variations on content about voting rules or voting sites).
- Evaluate how new product releases may affect the ongoing election and take appropriate action based on risk assessment and stakeholder input.