June 17, 2026

A Call to Tech Companies

Civil Society Urges Action to Prevent Platform Misuse Ahead of the Elections

To Tech Company Executives,

We, the undersigned organizations, write to raise concerns about how your services may be misused in ways that could undermine elections. As has been documented, AI tools can exacerbate many election challenges.[1] Recent eviscerations of settled election law and widespread redrawing of districts[2] has led to rampant confusion and heightened inquiry about where and how to cast a ballot, which means the risk for mis- and dis-information to thwart voters is also heightened. Now more than ever, AI developers and social media operators play pivotal roles impacting access to the ballot. Therefore, we are calling on tech companies to commit to the effective implementation of the following measures outlined herein to prevent misuse of your services:

- Develop Trust through Content Provenance and Labeling.
- Implement Election-Related Use Restrictions.
- Enable User Reporting and Enforce Policy Violations.
- Issue Periodic Transparency Reports.
- Limit AI-powered Cybersecurity Threats and Provide Resources for Election Security.
- Commit to the Tech Accord to Combat Deceptive Use of AI in Future Elections.

These measures are straightforward and familiar to many platforms and developers. They center the user experience in commonsense ways such as ensuring users know when content is generated or altered by AI. Some companies may have stated policies which comply with many of these measures. But policies are not enough. To rebuild public trust, companies must ensure effective implementation of features designed to prevent misuse of their services for mis/disinformation, cyberattacks, and other election-related harms; allow users to report any such misuse; and remove harmful or misleading content. Finally, we ask you to publicly commit to the measures you will take to prevent election-related harms, such as providing resources for

---

[1] Shanze Hasan, *The Effect of AI on Elections Around the World and What to Do About It*, Brennan Ctr. for Just. (June 6, 2024), https://www.brennancenter.org/our-work/analysis-opinion/effect-ai-elections-around-world-and-what-do-about-it .

[2] Hansi Lo, *How the Voting Rights Act ruling affects local redistricting*, NPR (May 16, 2026), https://www.npr.org/2026/05/18/nx-s1-5812837/supreme-court-voting-rights-act-state-local-redistricting.

users and election administrators, and issue public transparency reports outlining the election-related issues you identified on your platforms.

The decisions you make carry profound consequences for democratic participation in the U.S. Without proper guardrails, emerging technology has the potential to reinforce historic voter suppression tactics, especially those targeted at the Black community and other communities of color.[3] This includes the creation and proliferation of manipulated media that could mislead voters about the time, place, and manner of elections. We saw numerous such reports in 2024.[4] Although many platforms maintain policies around voting misinformation, such policies are only effective when they are enforced and when platforms consistently, and quickly, remove violative content. Alarmingly, several platforms have rolled back their election-related programs over the past year and a half, and are increasingly relying solely on measures like community notes instead of robust fact-checking, labeling, or content removal.[5] Research from the 2024 election highlights how these crowd-sourced tools failed to address the deluge of election-related falsehoods that flooded some platforms.[6] Furthermore, as people increasingly turn to chatbots for information, safeguards are critical to ensure chatbots do not provide misleading or incorrect election information.[7] Reports show chatbots are actively using false statements to persuade voters about candidates.[8] We share these issues because you are uniquely positioned to address them.

---

[3] Spencer Overton, *Overcoming Racial Harms to Democracy from Artificial Intelligence,* 110 Iowa L. Rev. 805 (2025); Jenna McLaughlin, *Racist texts bypassed some anti-spam protections after election*, NPR (Feb. 2, 2025), https://www.npr.org/2025/02/02/g-s1-41598/students-racist-text-messages-black-lgbtq-election.

[4] Maggie Astor, *Behind the A.I. Robocall That Impersonated Biden: A Democratic Consultant and a Magician*, N.Y. Times (Feb. 27, 2024), https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html; Shayan Sardarizadeh & Olga Robinson, *US officials say Russians faked 'Haitian voters' video*, BBC (Nov. 1, 2024), https://www.bbc.com/news/articles/c9vnyl2jnpjo.

[5] Isabel Linzer & Tim Harper, *Countdown to the Midterms: Social Media Platform Policies and the Information Environment*, Ctr. for Democracy & Tech. (Feb. 19, 2026), https://cdt.org/insights/countdown-to-the-midterms-social-media-platform-policies-and-the-information-environment/.

[6] Ctr. for Countering Digital Hate, Rated Not Helpful: How X's Community Notes System Falls Short on Misleading Election Claims 4, 18 (2024), https://counterhate.com/wp-content/uploads/2024/10/CCDH.CommunityNotes.FINAL-30.10.pdf.

[7] Garance Burke, *Chatbots' inaccurate, misleading responses about US elections threaten to keep voters from polls*, AP News, https://apnews.com/article/ai-chatbots-elections-artificial-intelligence-chatgpt-falsehoods-cc50dd0f3f4e7cc322c7235220fc4c69 (last updated Feb. 27, 2024).

[8] Sujata Gupta, *Chatbots spewing facts, and falsehoods, can sway voters*, Sci. News (Dec. 4, 2025), https://www.sciencenews.org/article/chatbots-facts-falsehood-sway-voters-ai.

Additionally, we are concerned about automated attacks on election security,[9] especially as officials adopt AI tools for election administration[10] and AI models are becoming more adept at identifying vulnerabilities.[11] We appreciate the efforts companies have made on this front by providing training and resources on election security to election administrators and want to reiterate that AI developers have an important role to play, especially given the reportedly weakened state of the Cybersecurity and Infrastructure Security Agency (CISA), a key resource for election security.[12]

As leaders who control the tools and platforms that can be misused against people ahead of the elections, we are calling on you to adopt the following commitments:

- Develop Trust through Content Provenance and Labeling. Companies that offer tools to create or modify content should ensure content includes durable, interoperable provenance measures, such as watermarks and the C2PA content credentials.[13] Platforms should identify such provenance data, as well as provenance data provided by a capture device, and add a clear label that content is AI-generated, AI-modified, or human-created as appropriate. Some platforms also provide users the option to limit AI-generated content shown in their feeds,[14] a promising development we encourage other platforms to adopt.

- Implement Election-Related Use Restrictions. Developers should include technical and policy restrictions on how their tools may be used for election-related materials. For example, chatbots should not respond to inquiries concerning the time, place, and manner of voting, or about voter registration and eligibility, and instead should redirect users to the official webpages of elections offices or trusted nonpartisan sources like the Election Protection Hotline.[15] Such restrictions should extend to any inquiries about elections or political candidates, and at a minimum, the chatbot should include clear

[9] Lawrence Norden & Gowri Ramachandran, *Artificial Intelligence and Election Security*, Brennan Ctr. for Just. (Oct. 5, 2023), https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-and-election-security
[10] *Artificial Intelligence (AI) and Election Administration*, U.S. Election Assistance Comm'n (Mar. 16, 2026), https://www.eac.gov/AI.
[11] Kevin Roose, *Anthropic Claims Its New A.I. Model, Mythos, Is a Cybersecurity 'Reckoning'*, N.Y. Times (Apr. 7, 2026), https://www.nytimes.com/2026/04/07/technology/anthropic-claims-its-new-ai-model-mythos-is-a-cybersecurity-reckoning.html.
[12] Zack Whittaker, *US cybersecurity agency CISA reportedly in dire shape amid Trump cuts and layoffs*, TechCrunch (Feb. 25, 2026), https://techcrunch.com/2026/02/25/us-cybersecurity-agency-cisa-reportedly-in-dire-shape-amid-trump-cuts-and-layoffs/.
[13] *Content Credentials : C2PA Technical Specification*, C2PA, https://spec.c2pa.org/specifications/specifications/2.3/specs/C2PA_Specification.html (last visited Apr. 13, 2026).
[14] Linzer & Harper, *supra* note 4.
[15] *Election Protection*, Lawyers' Comm. for C.R. Under L., https://866ourvote.org/ (last visited Apr. 13, 2026).

disclosures about the accuracy of its responses and urge verification through trusted sources. In addition, many developers have added limitations on the availability of their AI tools for creating or altering electoral content, particularly targeted campaign activities[16] and political ads.[17] We urge all developers to adopt such restrictions for electoral content or at least require labels to indicate that such content is AI-generated or modified as appropriate.

Similarly, online platforms should post public community guidelines that include clear prohibitions on posting false or misleading election information and guidance on how these policies will be enforced. Such election-related programs have been commonplace in recent years and therefore should be straightforward to enforce or reestablish.[18] Additionally, we urge platforms to return to professional fact-checking in the U.S., as studies have shown fact-checking to be more effective than community notes alone.[19] Where platform monitoring or moderation is done through automated means, we ask that you maintain human oversight over AI moderation to maintain platform trust.[20] Finally, we encourage platforms to implement heightened intervention protocols from 90 days prior to the general elections through certification of results and to commit to cross-platform collaboration to limit the spread of coordinated inauthentic behavior and synthetic content that can mislead voters.

- Enable User Reporting and Enforce Policy Violations. Companies that offer social media platforms or chatbots should include an easy-to-use reporting mechanism for users to report false or misleading information and other violations of platform policies as they relate to elections. The companies should also have public-facing policies on how they will respond to such reports, such as removing violative conduct or suspending accounts with repeated violations, and should consistently, and quickly, enforce such policies. Where a platform has other channels to report issues, such as for election administrators, information about those reporting channels should be publicly available.

---

[16] Tiffany Hsu & Cade Metz, *In Big Election Year, A.I.'s Architects Move Against Its Misuse*, N.Y. Times (Feb. 16, 2024), https://www.nytimes.com/2024/02/16/technology/ai-elections-defense.html.
[17] *Id.*; David Klepper, *Meta says it will begin labeling political ads that use AI-generated imagery*, AP News, https://apnews.com/article/meta-facebook-instagram-political-ads-deepfakes-2024-c4aec653d5043a09b1c78b4fb5dcd79b (last updated Nov. 8, 2023).
[18] Linzer & Harper, *supra* note 4.
[19] Dylan Walsh, *Online content moderation: What works, and what people want*, MIT Sloan (Mar. 31, 2025), https://mitsloan.mit.edu/ideas-made-to-matter/online-content-moderation-what-works-and-what-people-want.
[20] Maya Wiley, *An Open Letter to Tech Companies*, Leadership Conf. on Civ. and Hum. Rts. (Jan. 20, 2026), https://civilrights.org/resource/an-open-letter-to-tech-companies/#.

- Issue Periodic Transparency Reports. Many platforms already issue transparency reports that include information about enforcement of community standards. Such reports are important for public trust and research. We ask that all developers and platforms issue transparency reports before and after the November elections that include the following information:
    - Metrics on election-related issues identified and corresponding enforcement actions taken, disaggregated by reporting/monitoring channel (e.g., flagged by user report, flagged by automatic detection systems, etc.), specific policy or guideline violated, sub-category of issue, and language of reported content.
    - Metrics on how users engaged with the service on election-related issues, such as the number of queries for voting information and the most prevalent election-related queries.
    -
- Limit AI-powered Cybersecurity Threats and Provide Resources for Election Security. Many developers already prohibit the use of their tools for cyberattacks,[21] and we encourage all developers to adopt such a prohibition with technical and policy restrictions. In addition, we ask AI developers to provide cybersecurity support to election administrators, including through training, guidance materials, and technical support for any tools offered to administrators.

- Commit to the Tech Accord to Combat Deceptive Use of AI in Future Elections.[22] Ahead of the 2024 elections, twenty seven companies agreed to eight commitments designed to counter deceptive AI-generated content. Although implementation varied across platforms,[23] these commitments represented an important starting place for preserving fair elections in the age of AI. Significantly, these commitments embed cross-industry collaboration, which is needed to develop standards and methods to curtail the proliferation of false or misleading election information across platforms. Companies should commit, or re-commit, to these measures for future elections and provide public information on implementation.

We cannot ignore the inevitability of AI's influence on the future of democracy. Please let us know your availability to discuss how you are addressing the measures outlined herein. Our goal

[21] Cade Metz & Kate Conger, *A.I. Is on Its Way to Upending Cybersecurity*, N.Y. Times, https://www.nytimes.com/2026/04/06/technology/ai-cybersecurity-hackers.html (last updated Apr. 7, 2026).
[22] *A Tech Accord to Combat Deceptive Use of AI in 2024 Elections*, Munich Sec. Conf., https://securityconference.org/en/aielectionsaccord/accord/ (last visited Apr. 13, 2026).
[23] Abdiaziz Ahmed et al., *Tech Companies Pledged to Protect Elections from AI — Here's How They Did*, Brennan Ctr. for Just. (Feb. 13, 2025), https://www.brennancenter.org/our-work/research-reports/tech-companies-pledged-protect-elections-ai-heres-how-they-did;

is to work with you to advance these measures and ensure that AI tools are used to support free and fair elections for a pluralistic society.

Sincerely,

Lawyers' Committee for Civil Rights Under Law
Advancement Project
AFT
All Voting is Local
Asian and Pacific Islander American Vote (APIAVote)
Black Women's Roundtable
Clearinghouse on Women's Issues
Common Cause
Fair Elections Center
Feminist Majority Foundation
Hispanic Federation
Jewish Council for Public Affairs
League of United Latin American Citizens (LULAC)
Legal Defense Fund
National Action Network
National Association for the Advancement of Colored People
National Coalition on Black Civic Participation
National Council of Asian Pacific Americans (NCAPA)
National Urban League
National Women's Law Center
Stop AAPI Hate
The Leadership Conference on Civil and Human Rights
United Church of Christ Media Justice Ministry
Verified Voting