

BRENNAN CENTER FOR JUSTICE

October 16, 2023

Dear Chairperson Cushman, Member Duffie, Member Wiggins, and Executive Director Gay,

We understand that you are considering entering into a contract with EagleAI NETWORK, which has created a list-matching database (“EagleAI”). We urge you not to do so. EagleAI would add nothing to the already-active measures the state is taking to update its rolls; since 2019, the state has canceled or made inactive [hundreds of thousands](#) of registrants. Not only is EagleAI superfluous, it is flawed and unreliable. Its use may also, in some cases, run afoul of the National Voter Registration Act (“NVRA”), data privacy laws, the Computer Fraud and Abuse Act, and antidiscrimination law, among other potential issues. We urge you not to enter into any agreement with EagleAI and to reject any voter challenge derived from it.

I. EagleAI relies on sources that are not reliable for voter list maintenance.

As an initial matter, EagleAI cannot be [trusted](#) to provide reliable information regarding who on the voter rolls is not eligible to remain there. EagleAI relies solely on public information scraped from places like the National Change of Address database, criminal justice records, and property tax records. As we discussed in a [prior letter](#) to Georgia county election boards, these sources are insufficient to determine whether someone is still eligible to vote at their place of registration. For example, a military service member may want their mail forwarded while temporarily stationed outside of Georgia and eligible voters may be registered at a house they rent from someone else. Public documents and reporting have not shown that EagleAI has functionality to get around these shortcomings.

Even the voter rolls EagleAI relies on are likely not up to date. EagleAI is [reported](#) to be using the Voter Reference Foundation’s (“VoteRef”) publicly available voter list for its comparison. VoteRef is a snapshot of the voter rolls at the time VoteRef purchased them, so unless EagleAI is constantly buying new copies of the County’s voter rolls, these will quickly be out of date. VoteRef also lacks critical data like date of birth, which raises the risk of false matches based on name similarities. And EagleAI’s backers have made misleading statements about voter roll maintenance, such as a [claim](#) that there are more registered voters than residents in Georgia, which fails to take into account that the state has already moved many of these registrations onto its inactive voter list, where they are already on the path to being removed consistent with the requirements of the NVRA. As [summed up](#) by Georgia Elections Director Blake Evans, “EagleAI draws inaccurate conclusions and then presents them as if they are evidence of wrongdoing.”

In fact, EagleAI’s founder acknowledges that the data on their own do not provide a reliable basis for conducting voter list maintenance, instead [claiming](#) that the tool “simply points out

voter registrations that need to be reviewed by the election officials.” Yet when election boards have investigated similar information, it has proven to be a waste of their time. Last year Gwinnett County received a challenge to 37,000 names from VoterGA that relied on the same kinds of data used by EagleAI and derived from the same [network](#) of activists. The Gwinnett Elections Board undertook hundreds of hours of research into the voters. In the end, it did not remove a [single voter](#) from the rolls. For all the same reasons, EagleAI should never be used to verify voter registrations or resolve voter challenges; the data it relies on add nothing useful to the more-reliable information the Board already has.

Voter list maintenance is an important function of local elections administrators and we applaud your efforts to improve this process. But EagleAI will not further these goals. It offers nothing new from last year’s [failed](#) challenge efforts. It will point you towards false positives and waste your staff’s time. ERIC, of which Georgia is a member and which uses heavily encrypted, reliable identifying data, remains a far [better](#) tool for list maintenance.

II. EagleAI may violate privacy laws.

If this Board were to *share* data with EagleAI, that would raise data privacy concerns. Former Georgia State Election Board Chair William Duffey raised this issue in his May 11, 2023 [letter](#) to this Board, explaining that sharing voter information may violate Georgia law. The election code [specifies](#) that “original applications for voter registration [and] copies thereof” are not to be shared with the public, so the County cannot share those forms. And while the voter list is generally a public record, many components of individual entries are not, including bank statements, month and day of birth, social security numbers, emails, driver’s licenses, and location of registration.

This very data privacy issue sank the 2017 Presidential Advisory Commission on Election Integrity. The Commission asked states to turn over voter data including birth dates, justice system records, voting histories, and the final four digits of social security numbers. Many states [refused](#) to comply with the request, often because it sought non-public information that state law prohibited officials from sharing. Former President Trump – the Commission’s strongest backer – [admitted](#) that the inability to collect private voter data led to its demise. Contracting with groups like EagleAI is a known dead-end.

III. The Computer Fraud and Abuse Act may prohibit EagleAI from collecting certain data.

Not only would sharing voter information with EagleAI potentially violate privacy laws, but contracting with the group may expose the Board to liability if EagleAI is violating federal law or website terms of service. The [Computer Fraud and Abuse Act](#) is a federal law that imposes criminal and civil penalties on anyone who gains unauthorized access to a computer. Federal Courts have said that webscrapers like EagleAI are subject to the Act. In *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962 (N.D. Cal. 2013), a federal court in California ruled that Craigslist could sue 3Taps for using anonymous proxies to scrape classified ads off Craigslist. The parties agreed to a \$1 million settlement.

Additionally, while web scraping is legal, there are limitations on its use. Users of a website may consent to terms of service that prohibit scraping. Other websites may allow scraping but not commercial use of the data, such as selling a packet of information that includes protected IP (e.g., logos or databases). EagleAI would be using its data for a commercial purpose if it sold it to you. In other instances, scraping may scoop up personally identifiable information that is protected from disclosure. And, assuming EagleAI is built on an existing app development tool, it would need to purchase sufficient licenses so that every potential user of the platform is authorized to access it. Without extensive diligence to investigate these issues, this Board could be opening itself up to lawsuits and enforcement actions alongside EagleAI.

IV. The National Voter Registration Act and the Constitution limit when and how election officials may remove voters from the rolls.

In the event you did decide to use EagleAI, such use would need to be consistent with the NVRA, which both requires states (and their subdivisions) to perform voter list maintenance and places restraints on how they may do it.

Under the NVRA, states and their subdivisions can only [remove](#) voters in one of five circumstances. First, the voter asks to be removed. Second, if state law requires, for a criminal conviction or mental incapacity. Third, for the death of the voter. Fourth, if the voter confirms a change of residence in writing. Fifth, based on other evidence of a change of residence, but only after the state sends a notice and then the voter both fails to respond **and** does not appear to vote in the next two federal general elections. There is no exception for removing a voter for a change of residence because the county has used private data or because the voter was challenged.

We additionally caution that the NVRA prohibits the “systematic[]” removal of voters from the rolls within 90 days of a federal election. Voter removals derived from database matching are clearly systematic and therefore prohibited within that time-window.

The process protections in the NVRA exist alongside the constitutional requirement that individuals be afforded a meaningful hearing before being deprived of a protected interest. *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976). The Constitution also prohibits discrimination; the Equal Protection Clause of the Fourteenth Amendment protects against “laws singling out a certain class of citizens for disfavored legal status or general hardships.” *Romer v. Evans*, 517 U.S. 620, 633 (1996). EagleAI reportedly flags voters who are [registered](#) at homeless shelters or a nursing homes for investigation. These are vulnerable categories of voters and there is no evidence voters registered at these addresses are more likely to be ineligible. If EagleAI’s design disproportionately removes these voters from the rolls, it would be very difficult for this Board to deploy it in a way that does not discriminate against those voters.

We thank you for considering our position on this pressing issue. We would be happy to speak with you further about the concerns outlined above at your earliest convenience.

Sincerely,



Andrew B. Garber, Counsel

Co-signatories

ACLU of Georgia

Campaign Legal Center

League of Women Voters of Georgia

United to Protect Democracy

All Voting is Local Action

Coalition for the People's Agenda

New Georgia Project Action Fund