BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW

Voter Verification and Database Matching

Summary

- Ill-conceived state policies concerning HAVA’s statewide voter registration databases could keep hundreds of thousands of eligible voters off of the rolls, through no fault of their own.
- Database matching is unreliable.
- Inadequate matching standards are also responsible for improper purges.
- States can ensure that voter registration lists are as complete and accurate as possible while still safeguarding voters’ rights.
- Some states have adopted flexible matching standards for new registrants.
- Some states also have protective procedures in the event no match can be found.
- Flexible standards are good for new registrants – but not for purges of existing voters.
- Protecting legitimate voters also requires common-sense technological safeguards.

Ill-conceived state policies concerning HAVA’s statewide voter registration databases could keep hundreds of thousands of eligible voters off of the rolls, through no fault of their own. The Help America Vote Act of 2002 (HAVA) imposes a new procedural hurdle for voter registration. It requires that states try to match certain information in new voter registration forms against information in other state databases – like the driver’s license database of the motor vehicles department -- to verify its accuracy. The statute itself provides only one consequence for the match: if a registrant is a first-time voter who registered by mail and the state is able to match the information in her registration form, she is exempt from HAVA’s identification requirements; if not, she must provide ID or vote a provisional ballot. Some states, though, are adopting procedures that will keep voters off the rolls entirely if no match is found, by expressly conditioning registration on a successful match.

Database matching is unreliable. All state databases have errors -- typos, transposed names, and omitted information that could prevent matches from being found for eligible voters. Also, databases record information differently, which makes it even more difficult to find proper matches: “William” may not match “Will” or “Billy;” a “Jr.” and a “Sr.” may seem to be the same person; a maiden name may not match a married name. If the matching process is used to determine who may be registered – and therefore, who is eligible to vote – huge numbers of eligible citizens may be mistakenly disenfranchised. Even the most sophisticated matching technologies – which are not being used in most states – have a significant error rate. A sample run in New York City last year, for example, showed that if the right to vote were conditioned on a proper match, up to 20% of new voter registrations would have been rejected *solely* because of data entry errors.

Inadequate matching standards are also responsible for improper purges. Poor match standards may also lead to mistaken purges of eligible voters from the voter rolls. The infamous Florida purges of 2000 were caused in part by bad matching standards. Any Florida voter was purged from the rolls if his name shared 80 percent of the letters of a name in a nationwide felon database; a California felon named John Michaelson would cause an eligible Floridian named

John Michaels to be disenfranchised. Over half of the voters who appealed the purge after the 2000 election were deemed eligible.[1]

States can ensure that voter registration lists are as complete and accurate as possible while still safeguarding voters' rights. HAVA specifically leaves it up to the states to determine when a match is found and what to do if a state cannot match information provided by a person seeking to register as a voter. States can provide safeguards at both steps, to make the "verification" process a helpful tool rather than a barrier to voting.

Some states have adopted flexible matching standards for new registrants. States seeking to protect eligible voters have adopted procedures to maximize the chance that a match will be found for new voter registrants who are represented in other state databases. Delaware, for example, uses a "substantial match" standard based on the reasonable discretion of individual officials. Keeping standards flexible – and subject to human review – is a good way to compensate for typos, nicknames, and other common incongruities.

Some states also have protective procedures in the event no match can be found. Although some states take the untenable position that a voter is precluded from registering if the state cannot produce a match, many states do not attach such unwarranted consequences to a procedure that will frequently fail. Connecticut, for example, follows HAVA's guidance, by requiring that only in the event of a failed match must a first-time voter who registered by mail provide ID at the polls or vote a provisional ballot.

Flexible standards are good for new registrants – but not for purges of existing voters. Purges must also be conducted pursuant to transparent procedures that protect eligible voters. This means that a voter should be flagged as ineligible or removed from the rolls only when the state is *certain* that the voter in question is the voter whose eligibility is determined to be suspect – and then only pursuant to the procedures laid out in the National Voter Registration Act (NVRA). There should be redundant checks before a record is determined to be a duplicate or to belong to an ineligible voter; voters should be notified, with an opportunity to correct mistakes before any removal occurs; and most purges should be prohibited within 90 days of an election.

Protecting legitimate voters also requires common-sense technological safeguards. Many states are currently constructing large statewide voter registration databases for the first time. In addition to comprising the official list of voters – and thereby determining whether any individual is ultimately able to vote – the databases will also contain a substantial amount of private personal information. States must therefore implement common-sense technological protections for these enormous systems, such as requiring that a log of all database transactions be maintained, in order to track and remedy improper access. These databases must also be protected by layers of access and authorization, to ensure that only authorized transactions are made and only by authorized people.

[1] John Lantigua, *How the GOP Gamed the System in Florida*, NATION, Apr. 30, 2001, at 11.