Remarks of Wendy R. Weiser
Associate Counsel, Brennan Center for Justice at NYU School of Law

Before the
National Association of Secretaries of State

July 25, 2005

Since the theme of this panel is "community resources," I will begin by introducing the Brennan Center for Justice as a resource for election officials who want to enhance access to the franchise and voter participation. The Brennan Center is a non-partisan, non-profit law and policy institute. Our Democracy Program promotes election reforms that reduce barriers to full and equal political participation.

Our lawyers – often in collaboration with academics, scientists, and other experts – prepare a variety of legal and public policy materials on voting and election administration. We offer legal and policy counseling to state officials, and draft legislation, regulations and voter education materials. I encourage you to take advantage of our resources and assistance.

Another useful resource is the new National Network for State Election Reform, which is made up of dozens of voting rights and good government groups working to ensure that all eligible voters are able to cast meaningful ballots. Information about the Network is available outside.

Database Recommendations

I have been asked to address the Brennan Center's recommendations for implementing statewide voter registration databases. Our work has focused largely on HAVA's requirements that states *protect* voters' rights as they implement these databases, by providing adequate security and privacy protections, and ensuring that "the name of each registered voter *appears*" in the database, and that "*only* voters who are *not* registered or who are *not* eligible to vote are removed" from the database.

We have developed a number of legal and policy recommendations for HAVA-compliant databases, which are summarized in written testimony and comments we submitted to the EAC. These are available on our website at www.brennancenter.org. We urge you to consider these recommendations as soon as possible, and we are available to help you tailor these to your state.

Since time is short, I will address only a few of our recommendations.

Matching

One set of recommendations has to do with matching. There are several circumstances in which the records in voter databases may be subject to electronic matching – (1) when officials try to verify information in new registration forms; (2) when they look for duplicate records; and (3) when they engage in other list maintenance activities involving deaths, changes of address, or felony convictions.

The ability to do electronic matching can help improve list accuracy, at least with respect to those records for which officials are *able* to find matches.

But there is one essential fact about matching that must be kept in mind. Matching is notoriously *unreliable* – especially when dealing with personal data. Any typo or error in any database matched can lead to false results. And by all accounts the number of errors in the relevant databases is staggering. For example, one expert who audited DMV records in three states found that 30% of the addresses were incorrect.

False results can also come from matching algorithms that don't take into account *every* possible way personal data can be recorded. Data fields – like those for dates and addresses – are not standard across databases. And even where they are, the information inputted won't be consistent. "William" may not match "Will" or "Billy." "John Smith Jr." may seem to be the same person as "John Smith Sr." A matching protocol that does not check for transposed names may systematically fail to find matches for Asian-Americans. One that does not check maiden names may systematically exclude women. (Exact matches exacerbate these problems, missing from 30 to 70% of matches.)

In short, there are countless ways in which matching can go wrong. While states should use technologies that reduce common matching errors, there are major limits as to how much they can improve matching reliability.

This has serious implications for database policies. If matching is unreliable, then states *must* adopt other procedural safeguards for the franchise.

Verification

Let's start with the voter verification process. Recall that HAVA requires states to verify voter registration information against DMV and social security records. HAVA leaves it to states to determine *how* to conduct matches, and *what to do* if no match can be found. If the registrant is a first-time voter who registered by mail, and the state can*not* match her information, HAVA says that she must show ID before voting a regular ballot (but that she is still entitled to vote a provisional ballot). If the state *does* match her information, she is exempt from this ID requirement.

To ensure that voters are not deprived of the *benefits* of verification, states should adopt procedures that maximize officials' ability to find verifying matches and ensure that these procedures are uniform and open to public scrutiny.

But *more* importantly, states should *not* reject a voter registration application merely because of a match failure. A state that plans to reject such registrations is guaranteeing that *huge* numbers of eligible voters will be unfairly denied their right to vote.

New York City's recent experience shows the potential scope of the disaster that would ensue. Last September, the city's board of elections sent 15,000 registration records with driver's license numbers to the state DMV for verification. The DMV flagged over 3,500 of those records as listing driver's license numbers that did not exist in its database. The city board then undertook a massive audit of the voter database, reviewing the scanned original of each non-matching registration form. It found that election officials had incorrectly entered the driver's license numbers on almost 3,000 of those records – close to 20% of the total submitted. Had the city rejected those applications for failure to produce a match, almost 20% of new registrants who had supplied driver's license numbers would have been disenfranchised because of typos. This is precisely the kind of harm HAVA was intended to prevent.

States *should* adopt audit procedures like New York City's. But that won't entirely solve the problem. It is impossible to catch all errors by manually reviewing thousands of new registrations, often in very a short time period. And, audits of *voter* database records won't catch errors in the *matching* databases. The Social Security Administration estimated that at least 10% of attempts to match records with full social security numbers against its database will be inaccurate, and there is a significantly greater chance of error with so-called "foreign" or Latino names. It would be unacceptable for a state to make a voter's access to the franchise turn on these odds.

This is not only unfair; it also violates HAVA.

Purges

Bad matching procedures can also lead to unjust purges. An infamous example of this is the list of suspected felons Florida developed last year. The contractor that compiled that list did so by matching names on the voter list against records maintained by the department of corrections. For a match to be found, the contractor required matches in a variety of fields, including a field for race. The problem was that one database had a category for Hispanics and the other did not. The result was a list that systematically excluded Hispanics. And this wasn't the only matching failure: The purge list also contained a large number of voters who in fact *were* eligible to vote.

What does this mean for database policies?

A basic principle of fairness -- and of law -- is that a state must not deny a citizen her fundamental right to vote unless it is *certain* that she is *ineligible*. Purging, like access to registration, cannot be wholly dependent on unreliable results of matching.

In the purge context, this means that there should be uniform, non-discriminatory, and transparent standards for determining when a voter record is flagged for removal. It also means that, before removing a name from the list, states should notify the voter and provide her an opportunity to correct her record or demonstrate her eligibility. And, mass purges – including of duplicates – should not be done close to an election.

Security measures should also be built into database plans. As is done in the private sector, voter databases should keep detailed electronic records of all transactions, tracking when and by whom any changes or removals are made. They should be capable of generating reports of these transactions. And, there must be strict authorization rules, preventing unauthorized persons from accessing, destroying, or tampering with voter records.

For more recommendations on how to prevent unjust purges, I recommend an excellent report called *Purged*, by the ACLU, Demos and the Right to Vote Campaign, available outside.

Coordination and Privacy

I have a few quick additional points about database coordination.

Database coordination should be used not only for the purpose of verifying voters but also for correcting and updating voter records. Similarly, coordination with felony records should be used not only to determine who is ineligible to vote, but also to determine whose eligibility has been *restored* under state law.

Finally, states should adopt strong privacy protections to reduce the risk of identity theft and other privacy injuries. In particular, states should ensure that database coordination does *not expand* access to confidential voter information and is used *only* for verifying and updating voter records.

Backup Plan

I would like to end by noting that it is very likely that many new statewide databases simply will not work by the next federal election. We are informed that over half of the large IT projects undertaken every year fail. To prevent a large-scale election administration melt-down, please make sure that your state has back-up plans and procedures that do not depend on working databases.