The New York Times
nytimes.com

July 23, 2004

Insurance for Electronic Votes

This November, millions of voters will use electronic voting machines of questionable reliability. The election is by now too near for the sort of major overhaul that electronic voting requires. But there is still time for states and localities to protect the integrity of the voting and build public confidence in the results. The public should insist that election officials put these protections in place right away.

There has been extensive documentation of the problems with electronic voting. Several studies have found that it is vulnerable to vote theft and to inadvertent errors that can alter the outcome of an election. These inherent flaws are made worse by the reckless, and possibly illegal, actions of voting machine companies. This spring, California banned 14,000 Diebold voting machines because of allegations of "fraudulent actions" by the manufacturer.

In a well-run election system, electronic voting machines costing millions of dollars would not have been purchased before there were adequate standards for ensuring that they work properly. But given that nearly one-third of voters may be voting electronically this fall, it is fortunate that a number of private groups - including the Brennan Center for Justice at the New York University Law School and the Caltech/M.I.T. Voting Technology Project - have stepped forward with ideas for how election officials can minimize the risks. Kevin Shelley, the California secretary of state and a pioneer in the field, has also issued useful directives, many of which are on his official Web site.

Here are some things voters should demand:

Physical security for electronic systems Electronic voting machines must be kept secure at all times. It seems like an obvious point, but it's been ignored too often. In Georgia's March primary, voting machines were reported to have been delivered early to a polling place in a university student center, and left unattended. Some places start up machines the night before the election, a clear security risk.

The locks and antitampering devices on machines must be more secure. A study earlier this year in Maryland found, unbelievably, that all 16,000 electronic voting machines in the state had identical locks, which could be opened with a single key. The entire "chain of custody" of the voting, from the casting of ballots to the final tabulation, must be kept secure. Computers used in elections must not be used for anything else. All software used on them should be certified, and logs should be kept of everyone who has access to them.

Rigorous testing of electronic machines In many jurisdictions, testing is woefully inadequate. The machines should be exhaustively tested in advance, with real people casting votes, not simply machines "self-testing" their accuracy. The tests should use all of the ballot configurations that will be used in the election, and in large enough sample sizes to draw meaningful conclusions.

Randomly selected machines should be continually tested throughout Election Day. This "parallel monitoring," as it is known, can test parts of the system that come into play only during actual voting. It can ensure that no malicious software was installed that was designed to look honest before and after voting, but to steal votes during the election itself.

Properly trained poll workers, and rapid-response teams on Election Day Many of the problems that have occurred so far with electronic voting were due to election workers' errors. Poll workers must be extensively trained in the use of electronic voting machines, and given clearly written materials. On Election Day, there should be enough technology experts available to handle problems as they occur, monitoring teams doing spot checks for malfunctions and tampering, and rapid-response teams available for quick on-site visits.

Public records at the precinct level The more records that are created of vote totals, and the earlier in the process such records are created, the harder it is to steal votes. When the polls close, the results should be printed out and posted at each precinct and should remain there for at least one day to protect against alterations in the totals during transmission to the central office. Election results for precincts should also be immediately posted online.

The option to vote non-electronically Many voters do not trust electronic voting, and many are not confident of their computer skills. Any voter should be able to use a paper ballot. A review of Florida's primary this March found that elderly voters were more likely than others to cast ballots that did not select a candidate. Forcing people to vote electronically could lead to a rerun of the infamous "butterfly ballot" of 2000, with overly complicated voting technology that disenfranchises voters.

Independent security experts The short history of electronic voting has shown that manufacturers cannot be trusted when it comes to the reliability of their products. Jurisdictions that use electronic voting should employ outside experts to test their systems. These tests should be done well in advance and made public. Voters should be told what is being done to address any problems.

Transparency in electronic voting As we saw again this month in Florida, which was forced to scrap a flawed list of felons to be purged from voter rolls that it had originally kept from the public, secrecy in election administration is often a cover for incompetence, or even partisan manipulation. Voters should be able to monitor every aspect of electronic voting, from the purchase of machines to the final tabulation of votes, and offered enough training that they can understand what they are seeing.

In the long run, electronic voting should not be allowed without unimpeachable and mandatory security

standards, and machines that allow voters to see paper records and ensure that their votes are properly recorded. Unfortunately, a large part of the electorate will be using electronic machines this fall that lack these safeguards. Election officials have an obligation to act now to make the system as reliable as possible.

Making Votes Count: Editorials in this series remain online at www.nytimes.com/makingvotescount.