

Summary of the Problem with Electronic Voting

The 2000 presidential election and the consequential actions of Congress and the states are dramatically changing the American election process. The Help America Vote Act (HAVA) passed by Congress in 2002 mandates reform of the election processes of all states. Among its requirements are a revamp of the voter registration system, the replacement of all punch card systems, and the addition of electronic voting methods that allow disabled citizens to vote without assistance.

Two provisions that HAVA does not include are open-source software in electronic voting computers and a paper record of each ballot, verified by the voter at the time the ballot is cast. A great number of Americans are concerned that, because of the omission of these two provisions, the widespread changes now occurring are moving us toward less, rather than more, democracy.

We are gravely concerned about the increased reliance on voting machines that record and tally votes exclusively through secret electronic means and provide no paper ballot that can be verified by the voter. We have three major objections to entrusting our elections to these machines:

- ◆ Software errors are unavoidable.
- ◆ It is impossible to perform meaningful recounts to settle election disputes.
- ◆ The opportunities for fraud exist on a greater scale than ever before.

Software Errors

No one knows how to write bug-free software. This fact is not in dispute. The more complex the software, the more difficult it is to find and fix bugs. Election software is very complex, and it will contain errors, regardless of the skill and dedication of the engineers who design it and the programmers who code it.

As valuable as computers are, glitches are not uncommon. All of us who use computers know this. Undoubtedly, software errors will cause problems in future elections, just as they have in past elections. Here are three of the many examples of computer errors reported in local newspapers in recent elections:

Wake County, North Carolina, November 2002: flawed firmware caused 436 ballots to be lost. The vendor acknowledged responsibility and replaced the firmware.

Fairfax, Virginia, November 2003: testing ordered by a judge revealed that several voting machines subtracted one in every hundred votes for the candidate who lost her seat on the School Board.

Broward County, Florida, January 2004: 134 ballots were blank in a one-race election held on electronic voting machines. Florida law requires a count of the invalid ballots, but a recount was impossible because there were no ballots to recount.

These and many other reports of computer problems present us with an obvious question: how many election results were compromised by **unnoticed** computer errors and malfunctions? Of course, we have no way of knowing. These reported cases were detected, but it is only reasonable to assume there were other undetected errors, and we will never know how many.

Impossibility of Meaningful Recounts

When voting machines fail, manual recounts of paper ballots could provide correct results. But what if paper ballots are not available? The suspect election results in Broward County, Florida will stand, despite the fact that the election process did not comply with Florida law. Without paper ballots, the only alternative is to hold another election.

Trusting our votes to a wholly electronic process leaves us completely without recourse if that electronic process fails – and history shows that the process fails all too frequently. Without paper records that accurately reflect voters' choices, it is simply impossible to perform a meaningful recount. While voting computers can print a report of the votes cast, the report is simply a printout of the electronic records. If the initial tally is inaccurate, the report will also be inaccurate. This is not a meaningful recount.

Consider this very possible scenario, not unlike events that have occurred in past elections: A voter marks the appropriate locations on a computer screen, reviews the choices, and gives the command to cast the ballot. The computer records the ballot **incorrectly**. The voter leaves the booth, and at the end of the day, the poll worker prints out the ballot image. The voter's votes are incorrectly tallied, and the printed ballot is incorrect.

The computer error goes undetected because the voter is not there to view the printed version. The printout does not provide an audit trail appropriate for a meaningful recount; it is merely a printed version of the computer's inaccurate data.

Opportunities for Grand-Scale Fraud

Election fraud is not unknown in previous American elections, and it is not unexpected in future elections. However, the opportunities for fraud provided by electronic voting machines surpass all the opportunities available prior to the recent advances in technology. Here's what could happen:

An insider, working for one of the vendors of widely-used voting machines, could add malicious code to the software. That malicious code could alter the election results in every state that uses the voting computers, and the subversions could remain completely undetected. Here's why.

- 1) Computer hackers have the ability to create software that could alter election results in a way that would be subtle enough it would not set off any alarms in the minds of even the most observant election officials.
- 2) U.S. courts have ruled that the source code used to run voting machines is a "trade secret" and is not open to public scrutiny. So, malicious software could be clearly visible in the source code and yet remain hidden because no outside experts are allowed to inspect it.
- 3) The national standards for testing and certification are very weak and are not enforced. Testing is normally done by Independent Testing Authorities, in secret, and the results are not available to the public. Certification is provided by election officials who are not computer experts and usually know little about computer security or the intricacies of software.

Concerns about fraud are not simply speculation. A study by Johns Hopkins and Rice University computer experts revealed hundreds of security flaws in the software of a leading manufacturer. A separate study by SAIC confirmed the findings. A recent Ohio study of the four major voting machines has shown them all to be vulnerable to tampering. The study has prompted the Ohio Secretary of State to delay the installation of the machines until after the 2004 election.

A Reasonable Solution

Elections are everyone's business. Trade secrets and resistance to voters' needs are inappropriate when they pose a potential threat to democracy. If voting-machine manufacturers want to sell their products to American cities, counties, and states, let them be truly accountable to American voters. Let them provide each voter with a ballot that the voter can verify, that cannot be altered after verification, and that is available for a meaningful recount. Let them open their source code to the public so independent experts can inspect it and make public its strengths and weaknesses. The major manufacturers do not offer products that meet these requirements.

If the major voting machine manufacturers are not willing to be accountable to the public they claim to be serving, we must look elsewhere for the tools by which we can express our will in fair elections – tools that give us confidence in our continuing democracy. Voting machines that provide accessibility for the disabled and accountability to the public ARE available. Why are they not the equipment of choice?

The reasonable solution is for every state or the federal government to pass a law requiring all voting computers to provide a voter-verified audit trail and open source software. A bill (H.R. 2239 in the House and S. 1980 in the Senate) proposing such a law has been introduced into Congress. We must have these bills passed as soon as possible.