

## 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 the bugs. Election software is very complex, and it is certain to 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 them 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' coverage of previous 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

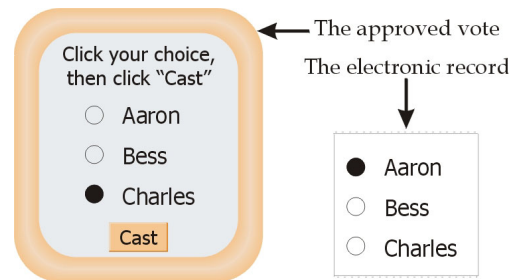
When voting machines fail, manual recounts of paper ballots could provide correct results. But what if paper ballots are not available? The suspect election results in Broward County, Florida will stand, despite the fact that the election process did not comply with Florida law. Without paper ballots,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

## Additional Resources

*Voter Confidence and Increased Accessibility Act of 2003 (H.R. 2239)*, introduced into the United States House of Representatives in May 2003, is an amendment to HAVA and requires voting computers to provide open-source software and a voter-verified paper audit trail. With 30 cosponsors, it still remains in the Committee on House Administrations. If it were passed, we would have the reasonable solution required by federal law. For more information, see <http://holt.house.gov/issues2.cfm?id=5996>.

*Analysis of an Electronic Voting System*, by Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan Wallach, was released July 24, 2003. The first three authors are at Johns Hopkins University; Wallach is at Rice). The authors have done a security analysis of Diebold code that was downloaded from an open FTP site earlier this year. While the paper is technical, significant portions of it can be read easily by a non-computer scientist. You can find the article at <http://avirubin.com/vote.pdf>.

*How to Build a Fraudulent Voting Machine*, by Steve Chessin. This brief, readable paper describes how to design a fraudulent voting machine that evades detection by the Independent Testing Authorities and local logic and accuracy tests. You can find the article at <http://www.zianet.com/leverett/chessin1.htm>.

*The Election Center Letter* by R. Doug Lewis and *Response to the letter* by Dr. David Jefferson is presented in the style of a debate, with Dr. Jefferson's responses interspersed with Mr. Lewis's attempts to defend the security and reliability of DRE voting systems (Direct Recording Electronic, often referred to as touchscreen systems). The article is at <http://verify.stanford.edu/EVOTE/ECresponse.html>.

*Resolution on Electronic Voting*. Nearly 1000 technologists and security experts across the United States have endorsed a resolution calling for a voter-verified audit trail on all election equipment. See the list at <http://www.verifiedvoting.org/endorsers.asp?catid=1>.

## Responses to Arguments for Wholly Electronic Voting

---

**Argument:** Touchscreens and other computerized voting machines have been operating successfully in elections for many years.

**Response:** How do we know the machines are "operating successfully"? Suppose they changed a few votes in every election. There is no way to check them independently, so how would we know? However, there are plenty of known problems. For example:

- ◆ 2002, Wellington, Florida. In a run-off election for a single city council seat, only two candidates were in the race, yet 78 votes were missing in the final tally of 1259 to 1263. There are only two possible explanations: Either 78 people went into the voting booth and didn't vote, or the Sequoia touchscreen machines didn't count those 78 votes. Without a paper backup, there was no way of finding out what happened to the votes.
- ◆ 2002, Union County, Florida, optical scan machines had been programmed to print out only the results for Republican candidates. Since the paper ballots were available, poll workers manually counted the 2700+ votes.
- ◆ 2000, Middlesex County, New Jersey. A Sequoia DRE machine was taken out of service after 65 votes had been cast. When the results were checked after the election, it was discovered that, out of those 65 voters, **no votes** were recorded for the Democrat and Republican candidates for one office, even though 27 votes each were recorded for their running mates. A representative of Sequoia insisted that no votes were lost, and that voters had simply failed to cast votes for the two candidates. Since there was no paper trail, it was impossible to resolve the question.

Disturbingly, when no paper ballots are available for recount, there is no way to know whether or not the outcome of the election was affected.

---

**Argument:** There have been no proven incidents of fraud involving DREs.

**Response:** But this is not evidence that there has been no fraud, since the methods for detecting and proving fraud have been systematically eliminated.

Incorrectly recorded votes cannot be detected because all recounts are based on the incorrect records. There is simply no way to know whether the votes recorded match the voters' intentions.

The software that records and counts the votes has been ruled a "trade secret" by the courts, thus it has been removed from public scrutiny. So, if any voting software did contain malicious code intended to pervert an election, there would be no way of finding out.

---

**Argument:** Testing will detect problems.

**Response:** It is very hard to find accidental errors by testing, and almost impossible to detect malicious code, which would be designed to evade detection. Note that all of the DRE problems mentioned above slipped past whatever testing was done. Steve Chessin has written a short description of "How to Build a Fraudulent Voting Machine." Computer security can dream up endless schemes for defrauding voting machines. [See <http://www.zianet.com/leverett/chessin1.htm>.]

---

**Argument:** FEC regulations and state certification processes ensure that the machines are reliable and secure.

**Response:** The regulations and their enforcement are totally inadequate for security. The FEC regulations are far weaker than security standards for other computer products. Conformance with the regulations is checked by a private "Independent Testing Authorities" (ITAs) overseen by a private organization (the National Association of State Election Directors). The reports on the system are secret, and it is very difficult to discover what the testing laboratories actually do.

The inadequacy of these processes was highlighted when Diebold accidentally released their software to the public. Computer security researchers at Johns Hopkins and Rice universities (<http://www.avirubin.com>) did a quick security review and immediately found glaring security flaws in the software. Obviously, the regulations and certification processes are failing to achieve even basic system security. By the way, according to Prof. Douglas Jones of the University of Iowa, the ITA reported that the Diebold system was the best they had ever seen.

---

**Argument:** DRE vendors claim that preserving the secrecy of their proprietary technology gives them an important hedge against being compromised.

**Response:** This argument - "security through obscurity" - has been disproven time and time again. Computer security researchers agree that, for a system to be secure, it must be designed to resist adversaries who know every detail about its inner workings. Besides, adversaries will always be able to acquire voting machines to tear apart and study (or a vendor may carelessly leave the software on a public web site, as did Diebold). Hackers may even be able to design "hacks" that modify voting machines after the machines are in use. Unless computers are secure against the people who know how they work, they are not secure.

---

**Argument:** The vendors have to escrow the source code of their systems with the Secretary of State's office.

**Response:** This might help, if experts were allowed to examine the source code if problems occurred in an election, but they aren't. In fact, it's not clear that there are any circumstances where the code can be examined. In cases where clearly flawed elections have been challenged in some states, the vendors and courts have refused to let independent experts look at the source code. Furthermore, the detailed reports from the certification authorities have also been protected by trade-secrecy, so even in a court proceeding it is impossible to check whether the equipment has been properly configured, and whether testing has been sufficient to assure confidence in its accuracy and reliability.

---

**Argument:** Voters with certain disabilities cannot verify paper ballots.

**Response:** Before the technology has been developed to solve this problem, there may be some voters who can cast a private ballot, but cannot verify that ballot. However, using this as an argument against having any voter verification is untenable. All voters, including those with disabilities, benefit from the increased election integrity that accompanies the requirement for verification by some voters. Furthermore, it is unreasonable to argue that beneficial features be removed because some voters cannot use them. For example, blind voters use audio interfaces which are slower and less convenient than touch screens, yet we do not ban the use of touch screens.