



THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

UPGRADE

The Boston Globe

It's the computers' turn to mess up elections

By Hiawatha Bray, 11/17/2003

Nearly a year before the presidential election, concerned citizens are already crying foul. But nobody's arguing over butterfly ballots or punch cards this time, as they did during the interminable Florida recount of 2000. All, it's the 21st century now. All future elections will be screwed up with the aid of computers. Various local elections throughout the United States early this month provided worrisome hints of the woes to come.

In Boone County, Ind., a high-tech voting machine counted 144,000 electronic ballots, in a precinct that contained fewer than 19,000 voters. In Fairfax County, Va., a Republican school board candidate lost by a handful of votes, then learned that at least one of the computerized ballot boxes had a glitch that may have subtracted some of her votes. "It's hard not to think that I have been robbed," the irate candidate told The Washington Post.

It wasn't supposed to be this way. Replacing punch cards with digital touch screens was supposed to deliver the accuracy we've learned to expect from computers.

Now that you've stopped laughing, you're probably all thinking the same thing. Anybody with a PC knows that computers can be wildly unreliable. What's being done to ensure that computerized voting systems are trustworthy?

Not nearly enough, according to the activists trying to force major modifications in digital voting systems. Bev Harris, author of the book "Black Box Voting," is the godmother of the movement. Harris said she's in favor of computerized voting, but not the way it's usually done.

"It's not a computing problem," said Harris. "It's an auditing problem."

The digital voting machines offer no independent way of double-checking the results they spit out at the end of the day. Election officials must simply take the machine's word for it. They're what engineers call a "black box," a device whose function isn't understood by those who use it.

One key reason is the secret software that runs the machines. Just as Microsoft Corp. owns Windows, Diebold Election Systems Inc. owns the code that runs its voting machines. That means the code is accessible only to its makers, and anyone with whom they might share it.

No big deal. Nearly all software is sold this way. But what if the secret code is insecure and badly written? When Johns Hopkins University computer scientist Aviel Rubin studied a leaked copy of Diebold's program, he was appalled.

"We found problems in the code that anyone who'd ever taken a single computer security course would have found," Rubin said. "I'd be willing to bet that the people who designed this system had no security expertise."

A study done for the state of Maryland by Science Applications International Corp. wasn't as scathing, but also found "a significant number" of security glitches.

So maybe the software shouldn't be secret. The Australian government has developed a digital voting system based entirely on open source software. All of the code is published so everybody knows exactly how it works. Voters who happen to be computer programmers can quickly identify glitches that could ruin an election.

But American voting machine makers aren't interested in sharing their software with rival firms.

"Our proprietary software is part of our company assets. It is something that we created," said Howard Van Pelt, CEO of Advanced Voting Solutions Inc., the Texas company whose machines were involved in the disputed Virginia election.

There's a better way to pry open the black box. All it takes is an old-fashioned ballot.

The concept is called voter verification. It would simply require that each machine would print a ballot after a voter has made his selections. The voter could then read the printout to ensure that he didn't somehow mistake Pat Buchanan for Al Gore, or vice versa. It'd be like double-checking your receipt at the supermarket checkout line.

Only this receipt doesn't get crumpled into a coat pocket. This one gets fed into an optical scanner at the polling place. The scanner records the votes on the printed ballot. At the end of the day, the tallies of the scanner and the touch screen computers are compared. They should match exactly. If they don't, you've got a boxful of paper ballots to recount.

Diebold spokesman David Bear said his firm is open to this idea.

"We do what our customers ask of us," he said. But will anyone ask? US Representative Rush Holt, a New Jersey Democrat, has offered legislation that would require all electronic voting systems to include voter verification, but there's little hope of passage anytime soon. It's certainly too late to affect the 2004 election.

The first generation of digital voting machines is already being deployed -- thousands of black boxes that may or may not work as intended. Get to bed early next Nov. 1. It could be a long Tuesday.

Hiawatha Bray can be reached at bray@globe.com.

© Copyright 2003 Globe Newspaper Company.

© [Copyright](#) 2003 The New York Times Company