Voting machine voodoo: Democracy at risk

By Colleen Redman

Online Journal Contributing Writer

November 19, 2003—I got my first taste of electronic voting on Election Day 2003. Although lever-voting machines were still being used in my county, a touch screen computer was available, and people lined up to try it.

I was surprised that no one I spoke to there was aware of the controversy surrounding electronic voting. No one seemed to know that computer scientists all over the country have warned that electronic voting is open to corruption, or that John Hopkins researchers studying the problem released a report on July 23 stating, "Our analysis shows that this voting system is far below even the most minimal security standards applicable to other contexts."

In the days following November 4, I looked through local town and city newspapers to see if any voting news stories would mention these concerns, but the stories I read were all about the novelty of the new touch screen machines, how easy they were to use, or how people are resistant to change.

Most Americans believe that the voting fiasco of the 2000 presidential election in Florida was caused by outdated voting practices. But this was only part of the problem. In a June 2001 article titled "Florida Vote Rife with Disparities, Study Says Rights Panel Finds Blacks Penalized," the Washington Post reported this: "Florida's conduct of the 2000 presidential election was marked by 'injustice, ineptitude and inefficiency' that unfairly penalized minority voters, the U.S. Commission on Civil Rights has concluded in a report that criticizes top state officials—particularly Governor Jeb bush and Secretary of State Katherine Harris—for allowing disparate treatment of voters." The article went on to cite the 167-page final draft report as stating that overzealous efforts to purge state voter lists was a factor in the widespread disenfranchisement of largely non-white voters.

Considering that many thousands of voters in predominately democratic precincts were either wrongfully removed from the Florida voter registration rolls or were turned away at the polls, one could conclude that this disenfranchisement played a large part in the outcome of the election.

Still, the hanging chads and butterfly ballots got the blame in Florida and officials scrambled to reform voting systems. Corporate venders and lobbyists swarmed Capitol Hill with promises that high tech computer voting was the way to reform. Congress passed the "Help America Vote Act" and allocated nearly $4 billion for new technology.

Corporations who manufacture the electronic voting systems, and benefit from mulit-million dollar contracts, have vigorously assured the public that their systems are secure. But academic researchers are not alone in their criticism of electronic voting. Recently, a military information technology contractor, SAIC, was commissioned by the State of Maryland to access the controversial touch screen voting machines and found them to be at "high risk of compromise." A private researcher inadvertently came across unprotected voting system files on the website of Diebold Election Systems, the leading voting machine manufacturer, and then posted them on the Internet to show how easy electronic voting is to corrupt (New York Times/John Schwarz/July 24 '03). The researcher, Bev Harris, author of "Black Box voting," reported that the files included diagrams of remote communications set-ups, passwords, encryption keys, source code, user manuals and more.

Although none of the local newspapers I read reported voter mistrust of electronic voting, a look at nationwide stories on the subject does indicate that public confidence in this voting process is eroding. An

October 31 Associated Press story by Robert Tanner, "Worries grow over new voting machines' reliability, security," lists the main concerns of electronic voting as: lack of confidence because there is no verifiable receipt of one's vote; inability to conduct a recount due to no physical record of the vote; and fear of election fraud, because the computers aren't secure enough, hackers can get in and manipulate election results.

Concerns about voter fraud could be more than theoretical. And even though computer technology is prone to shut down and error, electronic voting machines are already widely in use, and more are expected to be coming. Already there have been problems and conflicts of interest that raise suspicions.

Recently, the chief executive of Diebold unbelievably claimed that he was "committed to helping Ohio deliver its electoral votes to the president next year." (Newsweek/Steven Levy/November 3 '03). Former conservative radio talk-show host and current Republican U.S. Senator Chuck Hagel was also on the hot seat when it was revealed that, just prior to his senatorial campaign, he had ownership in the voting machine company that counted his winning votes (The Hill/January 29 '03) and did not disclose it.

Why were three Republican candidates in Canal County, Texas, declared victors in their respective races by the exact same margin of 18,181 votes? Why did Diebold post a California county's election tallies on its website before the polls closed (Associated Press/September 10 '03)? In Georgia it's been recently reported that Diebold installed patches on its voting machines before the state's gubernatorial election that were never certified by independent testing authorities (Wired.com/October 13 '03). In California, the state is launching an investigation into alleged illegal tampering with electronic voting machines in a San Francisco Bay area county (Associated Press/November 4 '03).

Since the SAIC findings, the same companies who assured us their voting systems were secure are now just as vigorously assuring us that they will fix the problems they insisted they didn't have. But should private corporate industries with possible vested interests in election results have such control over our most fundamental and essential democratic act? Should their computer programs that tell the voting machines how to tally votes continue to be allowed to be held as "trade secrets?" The computer voting industry is like a financial institution that doesn't keep records. Would we accept such loose standards from a bank that holds our money?

Representative Rush Holt is sponsoring legislation (HR 2239, the Voter Confidence and Increased Accessibility Act of 2003) that would require electronic voting machines to produce an actual paper record so that voters can verify their vote and election judges would have a paper trial to follow. I urge citizens of all political persuasions to contact their representatives and let them know they support this step in the right direction. I think we all should inform ourselves on the electronic voting issue and ponder what the John Hopkins study concluded: " . . . we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk.

Colleen Redman is a writer/poet living in the Blue Ridge Mountains of Virginia. She can be reached at joklein@swva.net.