THE CHRISTIAN SCIENCE MONITOR csmonitor.com

from the October 29, 2004 edition - http://www.csmonitor.com/2004/1029/p02s01-uspo.html

Nov. 2 the biggest test yet for touch-screen voting

Although some have raised concerns about votes being verified, others say special safeguards secure the system.

By Warren Richey | Staff writer of The Christian Science Monitor

Worried about your vote being counted on a computerized touch-screen machine in next week's election? Talk to Ted Selker.

The Massachusetts Institute of Technology professor is an expert in what can go wrong during elections. But touch-screen voting machines aren't high on his list.

While some computer voting specialists are sounding alarm bells about touch-screen voting and the need for printed paper trails, Professor Selker says the ATM-like machines are the safest voting method currently available. He adds that printout paper trails are vastly overrated.

"A lot of the reason paper ballots went away with [the introduction of] the lever voting machine was to get rid of people having their hands on paper, because paper can be destroyed, changed, replaced, or added to," Selker says.

As codirector of the Caltech-MIT/Voting Technology Project, Selker has spent much of the past four years studying the voting process from inside precinct polling places and election counting rooms.

In 2001, the Voting Technology Project issued a report estimating that 4 million to 6 million votes may have been lost nationwide during the 2000 election because of problems related to voter registration, ballot design and equipment, and polling-place operations. Similar problems will beset the 2004 election, but progress has been made, Selker says: "My prediction is that we will reduce the errors to less than half and maybe down to a fifth of the errors we had in 2000."

With early voting already briskly under way in several states, election officials are preparing for what is expected to be heavy voter turnout on Election Day. Of the top four voting methods, 35 percent of voters will cast their ballots on optical-scan voting machines, while 29 percent of voters will be using touch-screen systems. Fourteen percent will use lever machines, and another 14 percent will use punch cards.

Prominent among states still using punch cards is Ohio, a battleground state with high potential for postelection litigation. Following the 2000 election debacle, Florida replaced all its punch-card machines with touch-screen systems.

But questions have been raised about the reliability of such systems. Those concerns have been driven in part by news reports last year about close ties between Diebold Inc., a touch-screen manufacturer, and the Republican Party.

Rep. Robert Wexler (D) of Florida sued various state election officials to force them to purchase paper printers to provide a fail-safe backup system. Earlier this week, a federal judge in Fort Lauderdale threw out the case, ruling that the lack of printers did not violate constitutional principles of equal protection. But the judge acknowledged that as a policy matter, perhaps printers would be preferable.

Nevada is the only state to have uniformly equipped its touch-screen systems with printers. The system has been the subject of glowing press reports, but Selker says he monitored an election earlier this month in Reno, Nev., in which one out of every 20 printers jammed.

If election officials are properly trained and follow strict procedures, touch-screen systems can be safe and reliable without using paper. Selker says most systems have two internal hard drives and a detachable disk-drive ballot module.

Both the machine and the module contain their own records reflecting that machine's voting activity. So if someone were to steal the ballot module, a backup record could be obtained from the machine itself. In addition, this data can be compared against the number of signatures on the precinct voter rolls.

Selker says many election officials defeat the machine's primary safeguard by transporting the module and machine while they are still connected. If officials followed proper procedure and segregated the two right after the polls close, it would greatly increase the data's security.

Selker says by far the most serious concern over touch-screen systems is from a corrupt computer programmer trying to rig the voting machine to change the outcome of the election. But even this threat is easily neutralized, he says.

"You take your voting machine, you turn the clock to Nov. 2," he says. Then you run a test, with some individuals voting and others checking to see that the output and input match. "That is how you test it," he says. "Testing is completely crucial to anything working."

Selker says there is another way to significantly increase public confidence in touch-screen voting.

Rather than creating a paper trail using $1,000 printers, Selker designed a $80 voice-activated system that produces an audio transcript of every transaction on the voting machine.

Every touch-screen machine already has the capability of electronic audio: In effect, the machine can announce each candidate as votes are cast for him or her. If that audio is connected to an internal voice-activated tape recorder and a pair of headphones for the voter, individual voters would receive real-time verification that their votes for their favored candidates had been successfully made.

Selker says: "At the end of the day, if someone were to erase a portion of this - you remember the 18 lost minutes in the Nixon tapes - it is kind of noticeable."

Full HTML version of this story which may include photos, graphics, and related links .
