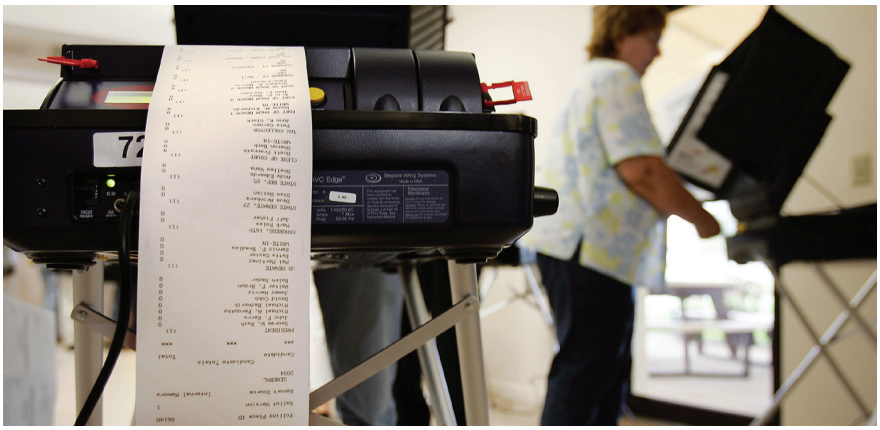
DOI:10.1145/1400181.1400192

David L. Dill

The U.S. Should Ban Paperless Electronic Voting Machines

Debating the public policy issues involved in proposed efforts toward improving voting systems while considering the range of technical and societal challenges.

Point: David L. Dill



PHOTOGRAPH BY MARIO TAMA

WHEN U.S. VOTERS go the polls next month, it will be impossible to determine whether the victorious candidates in many states were elected by a software bug, a virus in the voting system, the voting system programmers, or the voters themselves. Those states have voting machines that rely entirely on electronic ballots (these machines are referred to as direct-recording electronic voting machines, or DREs). There is no way to tell whether the votes recorded by DRE machines match those selected by the voters.

The solution is straightforward: Ban the use of untrustworthy paperless DREs, and demand that readily available systems that are auditable, accurate, reliable, accessible, and cost-effective be used in their place.

Paperless electronic voting is unworkable in principle with current technology. It is based on the mistaken idea that we can build computers that can be trusted to carry out operations whose results cannot be independently verified. But that's a practically impossible problem to solve, even given our best efforts. There is no way to know whether any of the many people involved in the design, implementation, and manufacture of the machines made a mistake or introduced a malicious change. If that were to happen, enough votes could be corrupted to change the outcomes of many elections—invisibly. This fact raises questions about all elections utilizing paperless DREs. Even if the machines are counting votes perfectly, we have no way of confirming that.

Why are paperless DREs more risky than the computers we rely on for banking, medical equipment, and flight software? It's because there is independent verification of the results of operating these other systems. If your plane lands in the wrong city or crashes, or your pacemaker malfunctions, either you or your survivors know about it. If banking software makes an error, you can check your statements to find it. But paperless DREs have no independent verification. If votes are changed in a plausible way, how will anyone ever know?

In reality, current DREs are not even close to "best efforts," as has been shown repeatedly, especially in the last year. Security reviews in California[a] and more recently in Ohio[b] documented breathtaking blunders in the security designs of the most widely used DRE systems in the U.S, which collectively process millions of votes. In each case, a single person with limited access could introduce a virus into the system during one election that could take over all the voting systems in the jurisdiction in the next election.[c]

It is urgently necessary to ban cur-

a M. Bishop, "Overview of Red Team Reports," Top-to-Bottom Review, California Secretary of State's Office; www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf.

b A press release on the EVEREST study of voting equipment security for the Ohio Secretary of State is available at www.sos.state.oh.us/SOS/PressReleases/2007. Detailed reports are available at www.sos.state.oh.us/SOS/elections/voterInformation/equipment/.

c There is a video of team at Princeton showing several ways to hack the Diebold AccuVote-TS DRE at youtube.com/watch?v=aZws98jw67g.

rent paperless DREs. Many states have already done so, but many states have not. All voters who go to the polls in Maryland and Georgia are forced to use paperless DREs, as are many voters in other states. Some other states are using paper ballots now, but could decide to convert to paperless e-voting in the future. Without federal legislation, voters in some states will be stuck with DREs for a long time.

Congress should mandate a specific class of paper trails: every voter should mark and cast a voter-verified paper ballot (VVPB). Each ballot can be counted by hand or scanned in the precincts by a scanner that checks it for overvotes or stray marks (the technical term for this type of system is precinct-count optical scan or PCOS). If there is a problem, the voter has a chance to fix the ballot or fill out a new one. Otherwise, the ballot is counted and deposited in secure ballot box. Or ballots can be counted by hand if desired. These systems can be made accessible to voters with a wide range of disabilities through the use of ballot-marking devices, which allow paper ballots to be read, marked, and verified via an accessible electronic interface.

Most studies have shown that PCOS systems are at least as accurate as any other voting system. They are less costly than touchscreen machines, and, if they fail, marked ballots can be stored in a ballot box and counted later. Most importantly, the hand-marked ballots can be verified and counted without having to trust computerized systems. Optical scan systems are already the dominant technology in the U.S.—they have been used for many years and the technology is steadily improving.

Some have argued that legislation requiring paper ballots would hamper innovation in voting technology. But the main problem in voting technology is not a lack of innovation, but how to prevent and recover from bad innovations.

Why paper and not some other permanent medium such as recordable compact discs? Paper can be read and written by people or machines, and, importantly, by (almost) everyone without machine assistance. Votes on paper cannot be removed or changed without detection. Critical documents on paper have been handled for many centuries and the procedures are easily understood by poll workers and election administrators. For example, it is easily recognized as a problem if a poll worker disappears into a back room for a few hours with a box of ballots.

Of course, simply using paper ballots does not guarantee election integrity. The ballots must be protected, and the processes for storing, transporting, handling, and counting them must transparent. Crucially, paper ballots enable the routine auditing of elections by choosing ballots from randomly selected precincts or machines and manually counting them to see if they match the machine totals.

Some have argued that legislation requiring paper ballots would hamper innovation in voting technology. But the main problem in voting technology is not a lack of innovation, but how to prevent and recover from bad innovations. State and local governments chose to purchase tens of thousands of DREs in spite of the dire warnings of computer technologists and activists—then the true risks of DREs turned out to be even worse than the warnings. The existing requirements and certification process did little to protect the voting system from this and other bad ideas.

A federal VVPB mandate would channel vendor R&D efforts into improving optical scan technology, instead of developing and marketing lucrative but ultimately dubious systems like DREs. If and when a radically new technology is proposed, the law can be changed—after a thorough debate about the true benefits, costs, and risks of that new technology—a debate that would have averted the disastrous experiment with DREs over the last few years. C

David L. Dill (dill@cs.stanford.edu) is a professor of computer science and electrical engineering at Stanford University and has been working actively on policy issues in voting technology since 2003.