

# Voting and Technology: Who Gets to Count Your Vote?

Paperless voting machines threaten the integrity of democratic process by what they *don't* do.



Voting problems associated with the 2000 U.S. Presidential election have spurred calls for more accurate voting systems. Unfortunately, many of the new computerized voting systems purchased today have major security and reliability problems.

The ideal voting technology would have five attributes: anonymity, scalability, speed, audit, and accuracy (direct mapping from intent to counted vote). In the rush to improve the first four, accuracy is being sacrificed. Accuracy is not how well the ballots are counted; it's how well the process maps voter intent into counted votes and the final tally. People misread ballots, punch cards don't tabulate properly, machines break down, ballots get lost. Mistakes, even fraud, happen.

When the election is close, we demand a recount. It involves going back to the original votes and counting them a second time. Presumably more care is taken, and the recount is more accurate.

But recounts will become history if paperless Direct Recording Electronic (DRE) voting machines—typically touch-screen machines—become prevalent. Approximately one in five Americans vote on such machines, as do citizens in several countries.<sup>1</sup> In the U.S. the “Help America Vote Act” will subsidize more DREs.

DREs have some attractive features. The human interface can be greatly improved. People with disabilities can vote unassisted. Ballots can be changed

at the last minute and quickly personalized for local elections.

However, all of the internal mechanics of voting are hidden from the voter. A computer can easily display one set of votes on the screen for confirmation by the voter while recording entirely different votes in electronic memory, either because of a programming error or a malicious design. Almost all the DREs currently certified by state and local agencies have an “audit gap” between the voter's finger and the electronic or magnetic medium on which the votes are recorded. Because the ballot must remain secret, there's no way to check whether the votes were accurately recorded once the voter leaves the booth; neither the recorded vote nor the process of recording it can be directly observed. Consequently, the integrity of elections rests on blind faith in the vendors, their employees, inspection laboratories, and people who may have access—legitimate or illegitimate—to the machine software.

With traditional voting machines, election officers are present to ensure integrity. But with DREs, election officers are powerless to prevent accidental or deliberate errors in the recording of votes. If there is tampering, it is likely present in the DRE's code, to which election officers have no access. In fact, DRE code is usually protected by code secrecy agreements, so that no one but the manufacturer has access to it. In recent cases the complainants have not been allowed to review the code, even when DRE-based elections have been contested in court.

Anyone who doubts the result of an election is now obliged to prove those results are inaccurate. But paper ballots—the main evidence providing that proof—are being eliminated. Vendors and election officials are free to claim that elections have gone

<sup>1</sup>For example, the U.K. recently conducted several local elections on the Internet. Internet voting raises additional security issues that space limitations preclude discussing in greater detail in this column.

“smoothly,” when there is, in fact, no evidence the votes counted had anything to do with the intent of the voters.

This is an unacceptable way to run a democracy. The voters and candidates are entitled to strong, affirmative proof that elections are accurate and honest. Paper-based elections with good election administration practices show the losers in an election that they lost fair and square. DREs do not.

Many voters and election officials are under the impression that computerized voting machines are

Even if adequate reliability and security were achievable, current practices are grossly inadequate. There is no indication that the major vendors or testing laboratories have computer security professionals to design and evaluate voting equipment. Manufacturers make basic computer security errors, such as failing to use cryptography appropriately, or designing their own home-brew cryptographic algorithms. Moreover, regulations and tests of greater rigor than those used for DREs routinely miss accidental flaws in software for other applications, and

---

## **Voters and candidates are entitled to strong, affirmative proof that elections are accurate and honest. Paper-based elections with good election administration practices show the losers in an election that they lost fair and square. DREs do not.**

---

infallible. DRE manufacturers insist that care goes into the design and programming of the machines. They and some election officials reassure us the machines meet rigorous standards set by the Federal Elections Commission; that the designs are reviewed and the machines thoroughly tested by independent testing labs; and that further review and testing occurs at the state and local levels.

The problem with these arguments is that it's impossible without some very special hardware (and maybe even with it) to make computers sufficiently reliable and secure for paperless electronic voting. The manufacturers attempt to hide this fact by keeping the designs of their machines a closely held secret, and then challenging critics to find flaws in those designs. Ironically, reverse engineering the code used for voting machines to check for bugs or voting fraud is likely to be a violation of the Digital Millennium Copyright Act.<sup>2</sup>

have virtually no chance of discovering tampering with software.

Problems are routine.<sup>3</sup> For example, a March 2002 runoff election in Wellington, FL, was decided by five votes, but 78 ballots had no recorded vote. Elections Supervisor Theresa LePore claimed those 78 people chose not to vote for the only office on the ballot! In 2000, a Sequoia DRE machine was taken out of service in an election in Middlesex County, NJ, after 65 votes had been cast. When the results were checked after the election, it was discovered that none of the 65 vote 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 top candidates. Since there was no paper trail, it was impossible to resolve either question.

---

<sup>2</sup>See [www.acm.org/usacm/Issues/DMCA.htm](http://www.acm.org/usacm/Issues/DMCA.htm) for information about ACM and USACM activities and statements relating to the DMCA.

<sup>3</sup>See the Q/A Web page at [verify.stanford.edu/evote.html](http://verify.stanford.edu/evote.html) and the wealth of information at [www.notablessoftware.com/evote.html](http://www.notablessoftware.com/evote.html).

While accidental design flaws are likely to cause election disasters in the immediate future, deliberate tampering is an even more serious concern. In older voting systems, election fraud typically is a labor-intensive process of altering or forging individual ballots. With large numbers of DREs in use, a small group or even a single individual at a voting machine manufacturer could alter software later installed on tens or hundreds of thousands of machines. If modified software switched a small percentage of votes between political parties, the tamperer could change the outcome of close races around the country.

There is nothing fundamental to DRE machines that requires an audit gap. The DRE machine simply needs to record the vote on paper when the voter has finished voting.<sup>4</sup> The voter reviews the paper ballot to verify it is marked in accordance with his or her intentions, after which the paper ballot is deposited into a ballot box. Discrepancies can be brought to the attention of an election official. The official vote count would be based on the DRE-produced paper ballots, with the DRE machine providing a preliminary total to be checked against the paper ballots in a recount. There is one such machine that is already certified in many states, and several of the major DRE vendors have agreed to provide voter-verifiable printers in contracts already in place.

Amazingly, the elimination of paper ballots is considered a major advantage by some, since the lack of paper simplifies the election process. The accompanying security risks are ignored, or even denied, by people who don't understand the underlying technology or simply want to believe the reassurances they receive from the vendors.


Maybe we will be extremely lucky, and every vote cast on DRE machines in the future will be accurately recorded. But there will always be surprising

election results, and people who question the results. Even if voting machines are accurate, it's important that voters trust the machines and *know* they are accurate. Democracy should not depend on blind faith.

The anonymity requirement of elections makes voting machines difficult to design and implement. You can't rely on a conventional audit, as we do with large-value financial computer systems.<sup>5</sup> Election machines must be treated like safety- and mission-critical systems: fault tolerant, redundant, carefully analyzed code. And they need to close the audit gap with paper ballots.

Over 900 computing professionals, including many of the top experts in computer security and electronic voting, have endorsed the "Resolution on Electronic Voting" petition,<sup>6</sup> urging that all DRE voting machines include a voter-verifiable audit trail.

Fortunately, some policymakers understand the security issues relating to voting. Rep. Rush Holt recently introduced the "Voter Confidence and Increased Accessibility Act of 2003" (H.R. 2239)<sup>7</sup> that calls for voter-verification and audit capacity in e-voting machines.

In 1871 William Marcy ("Boss") Tweed said: "As long as I get to count the votes, what are you going to do about it?" Paperless DRE machines ensure that only the company that built them gets to count the votes, and that no one else can ever recount them. 

---

**DAVID L. DILL** (dill@cs.stanford.edu) is a professor of computer science and, by courtesy, electrical engineering at Stanford University, Stanford, CA.

**BRUCE SCHNEIER** (schneier@counterpane.com) is CTO of Counterpane Internet Security, Cupertino, CA.

**BARBARA SIMONS** (simons@acm.org) is a former ACM president and current co-chair of ACM's U.S. Public Policy Committee.

---

© 2003 ACM 0002-0782/03/0800 \$5.00

---

<sup>5</sup>See [www.counterpane.com/crypto-gram-0102.html#10](http://www.counterpane.com/crypto-gram-0102.html#10) for more information.

<sup>6</sup>See [verify.stanford.edu/EVOTE/statement.html](http://verify.stanford.edu/EVOTE/statement.html) to read and endorse the petition.

<sup>7</sup>See [www.acm.org/usacm/PDF/HR2239\\_Holt\\_Bill.pdf](http://www.acm.org/usacm/PDF/HR2239_Holt_Bill.pdf)

<sup>4</sup>[www.counterpane.com/crypto-gram-0012.html#1](http://www.counterpane.com/crypto-gram-0012.html#1) is an early essay with this idea.