C. GARDNER/AP

# Ghosts in the machine

Electronic voting machines were supposed to vanquish unreliable counts. They did not — but **David Lindley** finds that other technologies present their own problems.

In the US mid-term election of 7 November 2006, the balloting in Sarasota County, Florida, was decidedly high-tech. Voters recorded their choices on electronic touch-screen machines that had been installed following the debacle of Florida's 2000 presidential race between Republican George W. Bush and Democrat Al Gore. Then, recounts and legal actions left the United States uncertain of its next leader for more than a month before Bush was eventually declared winner of the state — and the country — by little more than 500 votes out of almost 6 million. The devices promised to prevent a repeat of that event, memorable for its images of officials solemnly peering at hanging, pregnant and dimpled chads on punch-card ballots, trying to decide which of them to count as true votes. Surely with electronic voting, any such ambiguity would be impossible?

Evidently not. By the morning of 8 November, election officials were grappling with complaints about machine glitches, unrecorded votes and 'flipped' votes allocated to the wrong candidate. Somehow 13% of voters apparently failed to register any choice at all in the closely fought congressional race between Republican Vern Buchanan and Democrat Christine Jennings. By the time the protests and the lawsuits were over, and Buchanan was officially declared the winner by 369 votes, the conclusion was painfully clear: one set of problems had been traded for another.

The effort to reform US voting technology has not been successful. Florida, for example, threw out its old mechanical and paper-based voting technology after 2000, and switched to electronic systems, aided in part by funds allocated by the 2002 Help America Vote Act (HAVA). Critics of the move were quick to say that electronic voting machines were vulnerable to hacking and other attacks that could allow people to change the election results. And then experiences in Sarasota and elsewhere seemed to suggest that electronic machines could produce untrustworthy counts in many other ways.

As a result, Florida, New Mexico, Iowa and several other states have now rejected electronic voting and gone back to paper ballots that are marked by hand, typically by filling in a blank oval, and scanned by machine. But the cure may be worse than the disease — especially given the long history of paper ballots being lost, stolen, faked and stuffed into ballot boxes on the sly. "It's the most insecure medium there is," says Paul Herrnson, a political scientist at the University of Maryland in College Park.

R. WILSON/UNIV. MARYLAND

**"Paper is the most insecure medium there is."**
— Paul Herrnson

Meanwhile, some worry that arguments over the actual and alleged flaws of electronic voting systems have overshadowed more immediate concerns about usability and reliability. During the Florida 2000 election, for example, Palm Beach County's infamous 'butterfly ballot' — a split-page design with punch-card slots running down the middle — may have led a few thousand Gore supporters to accidentally vote for Reform candidate Pat Buchanan. Misleading ballot design, it seems, may also have caused problems in Sarasota.

Adding to the confusion is the fact that in the United States, conducting elections is the responsibility of state and local governments. The result is a patchwork in which nothing is standard or uniform, something that the HAVA legislation did little to change.

Voters heading to the polls on 4 November could face any number of glitches and anomalies, and the possibility that, once again, the outcome of a close presidential race could be shrouded in uncertainty.

## Universal problem

Controversies over electronic voting are not unique to the United States. The Netherlands embraced electronic voting in the 1970s, in part to deal with the complexity of the nationwide system of proportional representation by which members of parliament are elected. The Dutch system came into being before hacker culture was widespread, says Doug Jones, a computer scientist at the University of Iowa in Iowa City who has observed elections in the Netherlands. But in light of recent concerns, the country

has decided to return to paper balloting. Brazil, by contrast, introduced electronic voting beginning in 1996, and now has a fully electronic system. In the initial stages, as many as 7% of voters trying the new system were unable to record their choices electronically, but that figure fell to less than 0.2% by 2000, and the country remains committed to its voting technology.

Lingering memories of the 2000 election, along with the chance of a close contest on 4 November, make questions about voting technology especially urgent in the United States. The debate has been particularly contentious when it comes to direct recording electronic (DRE) devices, in which a voter's choice is translated immediately into electronic data. Sarasota's iVotronic voting machines —made by Election Systems & Software based in Omaha, Nebraska — generated no record of each vote other than the electronic data. (To satisfy a HAVA audit requirement, each one did print out a paper copy of its tally once the election was finished.) In Sarasota, therefore, there was "basically no evidence that could be examined after the fact that would explain what went wrong", says Jones.

**"Software fixes can really mess things up if you're making changes at the eleventh hour."**
— Avi Rubin

Concerns that DRE machines are vulnerable to undetectable tampering took off in 2003, when a group of computer scientists including Avi Rubin of Johns Hopkins University in Baltimore, Maryland, and Dan Wallach of Rice University in Houston, Texas, published a report (T. Kohno *et al. IEEE Symposium on Security and Privacy* 9–12 May 2004) pointing out serious security flaws in the software running the AccuVote-TS, a DRE system made by Diebold based in North Canton, Ohio. (A copy of the software had been posted on the Internet some months earlier.) As a safeguard against malfunction or tampering, the authors recommended that DRE systems should generate voter-verified paper audit trails (VVPAT) — literally, a paper display on which a voter could check that his or her vote had been cast correctly, and which could be kept as a record of the vote should any irregularities come to light.

Such a system was put in place in the May 2006 primary elections in Ohio, with printers being added to existing DRE systems. It was not a great success. A study commissioned by Ohio's Cuyahoga County found that almost 10% of the paper records were useless or absent, because, for example, the printers jammed, ran out of paper or overprinted. Ted Selker, who until June was at the Massachusetts Institute of Technology (MIT) in Cambridge as co-director of the California Institute of Technology/MIT Voting Technology Project, says that he saw similar problems when he observed elections in Nevada in 2004, one of the first occasions when a VVPAT system was added to electronic voting.

So a DRE device will record many legitimate ballots for which no paper record, or an illegible one, exists. That creates a further problem, says Michael Shamos, a computer scientist at the Carnegie Mellon University in Pittsburgh, Pennsylvania, who is also a lawyer. Election law generally states that the paper records, not the electronic data, constitute the legal ballot.

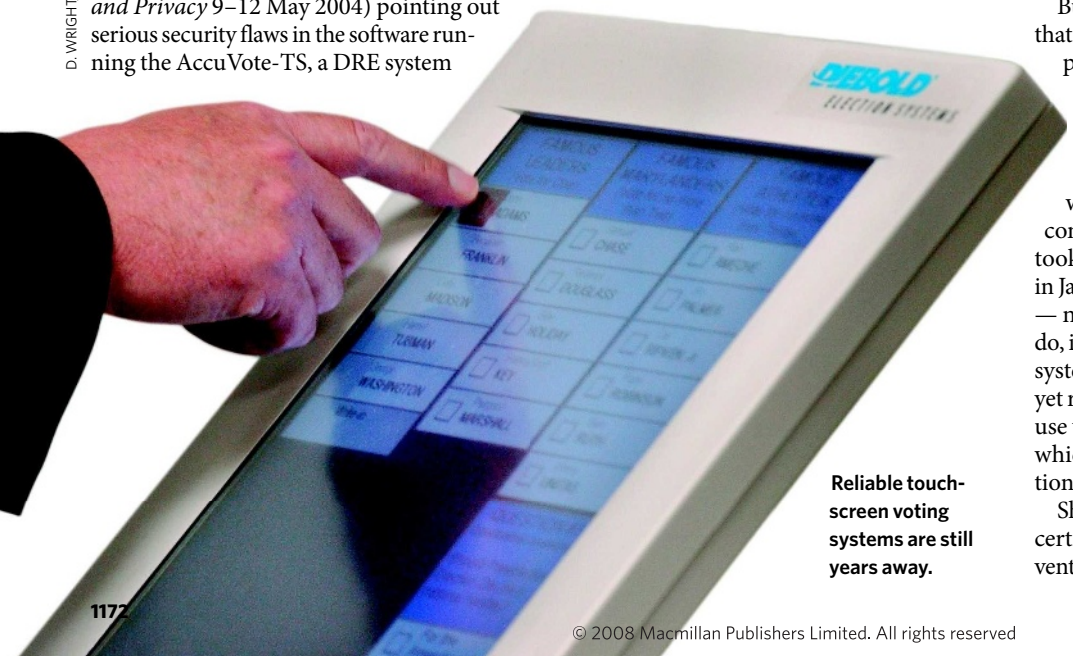
Although Rubin originally thought that adding VVPAT technology would make DRE systems workable, he now says that experience with paper-trail systems and poor implementation by the vendors has killed even that hope. And in any case, he says, VVPAT systems do nothing to solve the fundamental problem with electronic voting, which is that it depends on the reliability of software. Rubin says he is less concerned about external hacking or tampering than about software going wrong, or the risk of malicious actions from within voting-machine manufacturers. He is quick to add that he has never claimed that any manufacturer is corrupt, but thinks it's foolish to use systems that depend on them not being corrupt.

## Lost in the system

Mundane programming errors may present the main danger. In the March 2008 Ohio primary election, for example, poll workers found that votes were sporadically lost during the transfer of data from individual voting-machine memory cards to the central system; after discovering the problem, election officials were able to re-read the memory cards and establish the correct totals. At the time, Premier Election Solutions — the name under which the voting machine division of Diebold now operates — claimed that the data loss resulted from a software clash with an antivirus program on the central system. On 19 August, however, Premier acknowledged in a letter to Ohio secretary of state Jennifer Brunner that it had found an internal software bug that could cause votes to be dropped when data from two memory cards were being read at the same time. Election officials have now circulated guidelines to help poll workers to circumvent the problem without altering the voting equipment.

But even if Premier devised a software patch that repaired the glitch, says Shamos, the company couldn't install it without losing certification of its system for use in federal elections. The HAVA legislation vested authority for such certification in a new Election Assistance Commission (EAC), which issued revised guidelines for the conduct of elections in December 2005 and took over the federal certification procedure in January 2007. That certification is voluntary — not every state complies — but when they do, it is not a quick process. Of the eight voting systems currently under evaluation, none has yet received EAC certification. Systems now in use were accredited under the old procedure, which was overseen by the National Association of State Election Directors.

Shamos argues for an accelerated process to certify small changes, "especially when it prevents a much more serious problem". But Rubin




D. WRIGHT/AP

**Reliable touch-screen voting systems are still years away.**


Electronic voting has caused confusion for vendors, election officials and voters, but is it still more promising than paper?

J.-A. YANAK/AP G. CHAN/WPN/UPPA/PHOTOSHOT

thinks that is unrealistic. He says that even large software companies, despite all the testing and checking they do, keep releasing new versions of software as bugs and problems are fixed, and then the fixes give rise to new problems that require additional fixes. A quick turnaround is "an opportunity to really mess things up if you're making changes at the eleventh hour", he says.

The certification process also impinges on the question of software disclosure. Both critics and advocates of DRE systems generally argue that companies should make public the software they use, which would give them greater incentive to resolve security issues. Vendors can still protect themselves by patenting their ideas and holding copyright to their code, Wallach says, and disclosure should not generate security issues for well designed software. "Only if their systems are built like garbage does disclosure become a security problem."

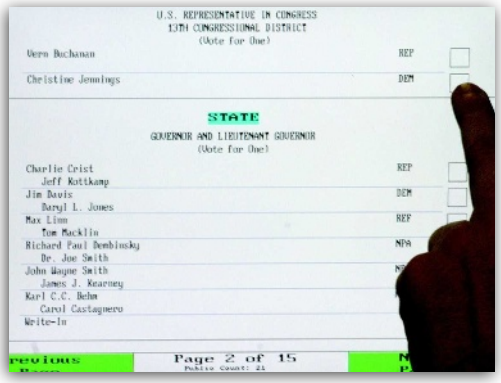
But then, as Rubin points out, voting-machine design "needs to be set in concrete in order to be certified". He imagines the case of a software security flaw or bug being discovered just before an election. "If you try to fix it, you will now be using an uncertified voting system and that would be an avenue for someone to tamper with the votes," he says, but if you don't fix it "you're going to use a system that you know is bad".

## Design errors

Another concern about voting machines is that they all too often neglect basic human factors. For example, use of a printed paper record tacitly assumes that a voter confronted with an incorrect paper ballot will reject it and ask to start again. But Selker says that in practice not many voters pay attention to the paper printout, or understand its purpose.

That conclusion is supported by Sarah Everett's PhD thesis at Rice University. Everett conducted mock elections to compare the performance of various voting technologies, including punch cards, paper ballots and a touch-screen interface designed by Wallach and his colleagues. In some experiments, deliberate errors — omitting an election race, or flipping a voter's selection — were introduced on the electronic system's final review screen, which subjects were asked to check before they cast their ballot. Almost all participants said that the review screen gave them more confidence that their votes had been correctly registered. Only about one-third of them, however, actually noticed that their votes had been changed.

Of course, Jones says, if even just a few people verify their vote, such review systems can still provide warning of systematic problems, as long as election officials act. In the Sarasota case, there was "ample evidence that something was wrong before polls officially opened". Difficulties with the machines were flagged by early voters, who under Florida law can vote ahead of election day, but their complaints brought no change in voting procedure.




The ballot design may have led some voters in Sarasota County to miss the congressional race at the top.

S. NESIUS/AP

The Sarasota 'undervote' came almost entirely from the 120,000 people who voted electronically, of whom almost 18,000 failed to register a choice in the Buchanan–Jennings congressional race. Among the roughly 20,000 absentee voters who sent in optical scan ballots, the undervote was a more typical 2.5%. Post-election testing by Florida officials and later by the Government Accountability Office produced no conclusive evidence of machine malfunctioning, although Wallach says that the tests did not address the full range of troubles that voters reported. "We have all kinds of evidence of touch-screen malfunction and miscalibration," he says. Touch screens must be calibrated so that they correctly connect the place where a voter touches the screen with the corresponding spot on the displayed ballot.

The *Sarasota Herald-Tribune*, however, suggested poor ballot design as another cause of the undervote. The Buchanan–Jennings race, in which there were no other candidates, appeared at the top of a screen, separated from the governor/lieutenant governor race by a blue banner. The suggestion was that a voter's eye would be drawn to the banner and the large race following it, and could easily overlook the smaller race at the top.

Selker tested this by running mock elections using the Sarasota ballot screens. He found that more than 16% of the test subjects missed the congressional race. When he put the race at the bottom of the previous page instead, almost 19% missed it.

Selker also has an explanation for the claims of vote flipping. He cites a study by Sarah Sled of the Caltech/MIT Voting Technology Project of the 2003 election that made Arnold Schwarzenegger governor of California. Of 135 candidates, only Schwarzenegger and two others got a substantial number of votes. The six candidates immediately above or below one of

J.-A. YANAK/AP



T. GANNAM/AP

Electronic votes are stored on memory cards before counting.

the three major candidates on the ballot did slightly but significantly better than the other minor candidates. Sled's conclusion was that about 0.4% of voters inadvertently voted for a candidate adjacent to their true choice.

Claims of vote flipping arise, Selker maintains, when voters mistakenly choose the wrong candidate and then, when they see a confirmation screen, assume that the machine has erred. But that's a point in favour of well-designed DRE devices, he argues: they give voters an immediate opportunity to review and correct their choices.

DRE systems are also easy to use. Herrnson and his colleagues conducted experiments in which volunteers worked through a moderately complex mock election on a variety of electronic systems, and with a hand-marked paper ballot. Volunteers rated the systems on a number of criteria, including ease of use, ability to correct a mistake and confidence that their choices were accurately recorded. Two of the three touch-screen systems got most of the high marks; the third scored less well largely because it jumped to the next screen without waiting for voters to signal that they were ready to proceed.

## Judged too early?

Shamos points out other advantages of DRE systems. They can more easily guide voters through complex ballots, can provide the ballot in a variety of languages, can adjust font sizes for voters with visual difficulties and are generally better for disabled voters. He says that the alarm raised over software security "was a perfectly good message, but it turned into a campaign of incredible vituperation against the concept of a computer being used in voting".

As a safeguard against the manipulation of electronic votes, Shamos says that the data representing the touch-screen image could flow directly into a non-rewritable recording medium. That record could be used to reconstruct the voter's operations on the touch screen.

Jones, however, is sceptical. Independent data capture has promise, he says, but "can you really show to me that it is independent?" What these systems aim to achieve, he says, is the electronic equivalent of a "camera over the shoulder", directly recording the voter's actions, but such techniques require data transfer and storage, and often end up being hackable themselves.

Apart from their technical challenges, proposals to improve security and provide trustworthy data back-up increase the cost of voting systems and make life more difficult for volunteer poll workers, whose training is often perfunctory. In addition, says Jones, election officials themselves are intimidated by novel equipment, and leave instruction and trouble-shooting to representatives of the vendor. Concerns over the expense of voting equipment, along with the uncertain legislative atmosphere, combine to make "a treacherous marketplace", says Peter Lichtenheld, a spokesman for Hart InterCivic in Austin, Texas, which makes both DRE and optical-scan voting systems.

There is still no sign of resolution. Critics of DRE systems concede that no voting system is perfect — but insist that electronic voting is uniquely susceptible to failures with catastrophic, system-wide consequences. Wallach argues, for example, that defrauding a paper ballot is labour-intensive, whereas for a hacker who has the ingenuity, and the means, to mount an attack on electronic systems, "the cost to throw an election is dirt cheap". But Herrnson counters that that distinction is not as stark as it might seem. Anyone wishing to throw an election the old-fashioned way would pick on close races and would know where tampering with a few ballot boxes would swing the result.

"Some of the critics of DRE voting machines uncritically recommend paper-ballot systems without understanding that they too have shortcomings," says Jones. Even so, he thinks that optically scanned paper ballots represent the best compromise. Paper ballots are easy to understand, he says, and although they are far from immune to fraud, "the frauds are understandable and the defences against the frauds are understandable".

> **"Paper-ballot systems also have shortcomings."**
> — Doug Jones

For now, Rubin endorses the same system, but "not because of some love for paper systems", he says. "It's just that I think DRE systems have too many inherent problems."

Florida has now embraced optically scanned paper ballots. But on 26 August, the *Sarasota Herald-Tribune* reported that a Premier scanner being used to read absentee ballots could not upload its data to the central tallying system, and vote totals had to be entered manually. And in the District of Columbia, which uses optical scanning technology from Sequoia Voting Systems, based in San Leandro, California, early vote counts in a 9 September primary election for the city council were inflated by thousands of phantom votes that disappeared in subsequent election reports. The cause of the problem has not been definitively identified.

Moreover, Herrnson warns, the return to paper ballots inevitably raises the spectre of a repeat of Florida 2000, with a close result spawning unresolvable arguments over what does and does not constitute a legitimate mark. In place of the relentless focus on the flaws of electronic voting, he says, what is needed is a dispassionate comparison of voting systems taking security, reliability and usability into account. "The debate would benefit from a panel of election administrators and computer people who aren't bound to one position," he says. What's also needed, says Jones, is patience. In recent years, the discovery of electoral flaws has led to "irresponsible and unrealistic" expectations that new and better equipment can be put into place in a matter of months. Vendors need two years to develop voting systems to meet new standards, he says, and election officials need another two years to get the systems working reliably.

That kind of time might be available — as long as this November's election doesn't end in contention and acrimony. ■

**David Lindley is a freelance science writer based in Alexandria, Virginia.**

**See Editorial, page 1149.**