

**ELECTRONIC VOTING MACHINES PROMISE TO MAKE**

**FIXING**

**ELECTIONS MORE ACCURATE THAN EVER BEFORE, BUT**

**THE**

**ONLY IF CERTAIN PROBLEMS—WITH THE MACHINES**

**VOTE**

**AND THE WIDER ELECTORAL PROCESS—ARE RECTIFIED**

By Ted Selker

Voting may seem like a simple activity—cast ballots, then count them. Complexity arises, however, because voters must be registered and votes must be recorded in secrecy, transferred securely and counted accurately. We vote rarely, so the procedure never becomes a well-practiced routine. One race between two candidates is easy. Half a dozen races, each between several candidates, and ballot measures besides—that’s harder. This complex process is so vital to our democracy that problems with it are as noteworthy as engineering faults in a nuclear power plant.

Votes can be lost at every stage of the process. The infamous 2000 U.S. presidential election dramatized some very basic, yet systemic, flaws concerning who got to vote and how the votes were counted. An estimated four million to six

million ballots were not counted or were prevented from being cast at all—well over 2 percent of the 150 million registered voters. This is a shockingly large number considering that the decision of which candidate would assume the most powerful office in the world came to rest on 537 ballots in Florida.

Three simple problems were to blame for these losses. The first, which made up the largest contribution, was from registration database errors that prevented 1.5 million to three million votes; this problem was exemplified by 80,000 names taken off the Florida lists because of a poorly designed computer algorithm. Second, a further 1.5 million to two million votes were uncountable because of equipment glitches, mostly bad ballot design. For example, the butterfly ballot of Palm Beach County confused many into voting for an unintended candidate and also contributed to another appalling outcome: 19,235 people, or 4 percent of voters, selected more than one presidential candidate. Equipment problems such as clogged punch holes resulted in an additional 682 dimpled ballots that were not counted there. Finally, according to the U.S. Census Bureau, about one million registered voters reported that polling-place difficulties such as long lines prevented them from casting a vote.

Thus, registration and polling-place troubles accounted for about two thirds of the documentable lost votes in 2000. The remaining one third were technology-related, most notably ballot design and mechanical failures. In the aftermath of the 2000 election, officials across the country, at both the federal and local levels, have scrambled to abandon old approaches, such as lever machines and punch cards, in favor of newer methods. Many are turning to electronic voting machines. Although these machines offer many advantages, we must make sure that these



VOTING MACHINE—here, Sequoia Voting Systems' Edge AVC Edge (right)—is fairly typical of direct record electronic (DRE) voting machines on the market. Voters enter their votes via a touch-screen interface (left; screen shot from TK TK).

new systems simplify the election process, reduce errors and eliminate fraud.

Some countries have introduced electronic systems with great success. Brazil started testing electronic voting machines in the mid-1990s and since 2000 has been using one type of machine across its vast pool of 106 million voters. It has multiple organizations responsible for different aspects of voting equipment development as part of the safeguards. It also introduced the machines in carefully controlled stages—with 40,000 voters in 1996 (7 percent of whom failed to record their votes electronically) and 150,000 in 1998 (2 percent failure). Improvements based on those experiments reduced the failure rate to an estimated 0.2 percent in 2000.

## Voting Technology

VOTING SYSTEMS have a long history of advancing with technology. In ancient Greece, Egypt and Rome, marks were made for candidates on pieces of discarded pottery called ostraca. Paper superseded pottery in the hand-counted paper ballot, which is still used by 1.3 percent of U.S. voters. Other modern technologies are lever machines, punch cards and mark-sense ballots (where each candidate's name is next to an empty oval or other shape that must be marked correctly to indicate the selection, and a scanner counts the votes automatically). The table on pages 94 and 95 summarizes the benefits and drawbacks of each of these methods and suggests ways to improve them. A lengthier discussion of nonelectronic systems is at [www.sciam.com/ontheweb](http://www.sciam.com/ontheweb).

Electronic voting machines have been around for 135 years—Thomas Edison patented one in 1869. Elections started testing electronic voting machines in the 1970s, when displaying and recording a ballot directly into a computer file became economical. At first, many were mixed-media machines, using paper to present the selections and buttons to record the votes. Officials had to carefully align the paper with the buttons and indicator lights. Electronic voting machines that use such paper overlays are still on the market. More modern Direct

Record Electronic (DRE) voting machines present the ballot and feedback information on an electronic display, which may be combined with audio.

Such machines have many advantages: they can stop a voter from choosing too many candidates (called overvoting), and they can warn if no candidate is picked on a race (undervoting). For instance, when Georgia changed over to DREs in 2002, residuals (the total of overvotes and undervotes combined) were reduced from among the worst in the nation at 3.2 percent on the top race in 2000 to 0.9 percent in 2002. So-called ballotless voting allows the machines to eliminate tampering with physical ballots during handling or counting. (Lever machines, dating back to 1892, share many of those features.)

Yet the birthing of DRE voting equipment in the U.S. has not been easy. The voting machine industry is fragmented, with numerous companies pursuing a variety of products and without a mature body of industry-wide standards in place. Deciding what is a good voting machine is still being discussed by various advocacy organizations and groups such as the IEEE Project 1583 on voting equipment standards. Allegations of voting companies using money to influence testing and purchasing of equipment are not uncommon.

Complicating matters, local jurisdictions across the country have different rules and approaches to testing and using voting equipment. Some counties, such as Los Angeles, are sophisticated enough that they commission voting machines built to their own specifications. Many other municipalities know so little about voting that they employ voting companies to run the election and report the results.

Polling-place practices add further hazards of insecurity and potential malfunctions. I recall walking into the central election warehouse (where the voting machines are stored and the precinct vote tallies are combined) in Broward County, Florida, when it was being used for a recount in December 2002. The building's loading dock was opened to the outdoors for ventilation. The control center for tallying all the votes was a small computer room; the door to that room was ajar and no log was kept of personnel entering and leaving.

Beyond external issues, DRE machines themselves have had technological shortcomings that have slowed their adoption. Voters have found their displays confusing or challenging to use. Software bugs and difficulties in setting up DREs have also presented problems. During the 2002 Broward County recount, I was allowed to try out machines from Electronic Systems and Services (ESS), one of the country's major election machine makers. The ESS machines had an excessive undervote because the "move to next race" button was too close to the "deposit my ballot" button. An audio ballot was so poorly designed it took about 45 minutes to vote.

On machines made by the company Sequoia, people who chose a straight party vote and then tried to select that party's presidential candidate were unaware that they were *deselecting* their presidential choice. A massive 10 percent undervote was registered in one county using Sequoia machines in New Mexico.

Examining the insides of new voting machines still reveals

## Overview/*Electronic Voting*

- Following the infamous 2000 presidential election, electoral officials around the country have scrambled to upgrade their voting technology with newer systems, such as direct record electronic voting machines (DREs).
- A state or county that is considering buying DREs, should hire experts to test the machines thoroughly for bugs, malicious software and security holes and to assess the quality of the user interface.
- Election officials and polling-place workers should be well versed in the operation of their machines and should follow practices that do not compromise the security of the vote.
- In addition to these technology-related issues, the voter registration process and polling-place practices in general must be improved to prevent massive losses of votes.

## AUDIT TRAILS

An audit trail printed on paper or recorded on tape or CD would enable an independent recount of votes made on an electronic voting machine.

**1** Voter makes selections using a touch screen.

**2** Audio confirmation of votes made is played to the voter over headphones.



**3** A tape recorder also records the audio confirmations, providing a permanent human- and machine-readable audit trail for the votes.



**VERIVOTE PRINTER UPGRADE** to Sequoia Voting Systems' AVC Edge voting machine produces a paper copy of the votes made on it and displays it behind a window. Before leaving the voting booth, the voter can verify her vote by inspecting the paper record, which is retained by the machine for use in recounts.

many physical security faults. For example, some machines have a lifetime electronic odometer that is supposed to read every vote that the machine makes. But the odometer is connected to the rest of the machine by a cable that a corrupt poll worker could unplug to circumvent it without breaking a seal.

Source code for voting machines made by different companies, like most commercial software, is a trade secret. Election machine companies allow buyers to show the source code to experts under confidential terms. Unfortunately, the local election officials might not know how to find a qualified expert. And when they find one, will the voting companies be required to listen? For instance, in 1997 Iowa was considering a voting machine made by Global Election Systems, which was later bought out by Diebold. Computer scientist Douglas W. Jones of the University of Iowa pointed out security issues, and the state bought Sequoia machines instead. In February 2003

Diebold left its software on unsecured servers, and DRE critics posted Diebold's code on the Internet for everyone to see. The problems that Jones saw six years earlier had not been fixed. Any person with physical access to the machines and a moderate amount of computer knowledge could have hacked into them to produce any outcome desired.

The best computer security available depends on sophisticated encryption and carefully designed protocols. Yet to know the system has not been compromised requires testing. DRE machines have not received the constant testing that they require. Security of today's voting machines is wholly dependent on election workers and the procedures that they follow.

Because virtually all tallies, no matter what voting method is used, are now stored and transmitted in some electronic form, computer fraud is possible with all voting systems. The advent of DRE machines potentially allows such tampering to go

## EXISTING VOTING TECHNOLOGIES

Improving or optimizing an existing technology may be a better choice for many counties than hasty adoption of a new system—introduction of a new technology is often accompanied by an increase in errors.

TECHNOLOGY	Hand-counted paper ballots	Lever machines	Punch cards
COMMENTS	<ul style="list-style-type: none"> <li>Used by 1.3 percent of U.S.</li> </ul>	<ul style="list-style-type: none"> <li>First used in 1892 in Lockport, N.Y.</li> </ul>	<ul style="list-style-type: none"> <li>First used in 1964 in Fulton and De Kalb counties, Georgia</li> </ul>
ADVANTAGES	<ul style="list-style-type: none"> <li>Simple</li> <li>Lowest residual* rate</li> </ul>	<ul style="list-style-type: none"> <li>Overvotes<sup>†</sup> are impossible</li> <li>Guarantees secrecy of vote</li> </ul>	<ul style="list-style-type: none"> <li>Removes human errors of tallying</li> <li>Compact machines</li> </ul>
DISADVANTAGES	<ul style="list-style-type: none"> <li>Recounts differ from original count by twice as much as machine-counted votes do</li> <li>Persistent allegations of votes being altered, added, lost, and so on</li> </ul>	<ul style="list-style-type: none"> <li>Bulky, massive machines</li> <li>Defective odometers: common</li> <li>Misreading of odometers</li> <li>Voting falloff on lower races (for Senate, state office, for example)</li> </ul>	<ul style="list-style-type: none"> <li>Hard to punch holes correctly</li> <li>Often punch wrong hole</li> <li>Ballot design troubles</li> <li>Card readers jam frequently</li> </ul>
WAYS TO IMPROVE	<ul style="list-style-type: none"> <li>Count by mechanical scanner</li> <li>Treat paper with light, heat or coating material to make vote indelible</li> </ul>	<ul style="list-style-type: none"> <li>Check and service before each election</li> <li>Monitor odometers with video cameras</li> <li>Improve labeling of groups of levers forming a race</li> <li>Adjustable height of machines</li> </ul>	<ul style="list-style-type: none"> <li>Optical way to check ballot while in booth might help</li> </ul>

unchecked from the point at which the voter attempts to cast a ballot. Schemes for altering ballots have always existed, but a computerized attack could have widespread effect were it waged on a large jurisdiction that uses one kind of software on one type of machine. Using a single system allows large jurisdictions to get organized and improve their results but must be accompanied by stringent controls.

The successful reduction of residuals across all of Georgia, mentioned earlier, is a case in point. Thorough tests on the DREs at Kennesaw State University found many problems, which were resolved before the machines were put into use. This rigorous testing and careful introduction of the machines were central to the state's success.

### Electronic Fraud

HOW CAN WE FIND all the dangers created by bad software and prevent or correct them before they compromise an election? Reading source code exposes its quality and its use of security approaches and can reveal bugs. But the only completely reliable way to test software is by running it through all the possible situations that it might be faced with.

In 1983 Ken Thompson, on receipt of the Association for Computing Machinery's Turing Award (the most prestigious award in computer science), gave a lecture entitled "Reflections on Trusting Trust." In it he showed the possibility of hazards such as "Easter eggs"—pieces of code that are not visible to a reader of the program. In a voting machine, such code would do nothing until election day, when it would change how votes were recorded. Such code could be loaded into a voting machine in many ways: in the voting software itself, in the tools that as-

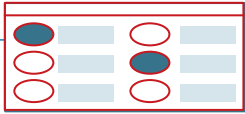
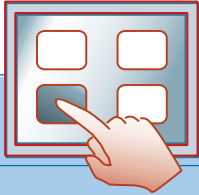
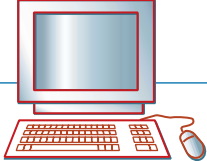
semble the software (compiler, linker and loader), or in the tools the program depends on (database, operating system scheduler, memory management and graphical-user-interface controller).

Tests must therefore be conducted to catch Easter eggs and bugs that occur only on election day. Many electronic voting machines have clocks in them that can be set forward to the day of the election to perform a test. But these clocks could be manipulated by officials to rerun an election and create bogus voting records, so a safer voting machine would not allow its clock to be set in the field. Such machines would need to be tested for Easter egg fraud on election day. In November 2003 in California a random selection of each electronic voting system was taken aside on the day of election, and careful parallel elections were conducted to show that the machines were completely accurate at recording votes. These tests demonstrated that the voting machines were working correctly.

To prepare for a fraud-free voting day requires that every effort be made to create voting machines that do not harbor malicious code. The computer science research community is constantly debating the question of how to make provably secure software. Computer security experts have devised many approaches to keep computers reliable enough for other purposes, such as financial transactions. Financial software transfers billions of dollars every day, is extensively tested and holds up well under concerted attacks. The same security techniques can be applied to voting machines. Some researchers believe that the security precautions of "open source" (making the programs available for anyone to examine) and encryption techniques can help but not completely guard against Easter eggs.

Guarding votes against being compromised has always re-



 <b>Mark-sense ballots</b>	 <b>Electronic machines</b>	 <b>Internet voting, phone messaging, interactive TV</b>
<ul style="list-style-type: none"> <li>■ First used in 1962 in California</li> </ul>	<ul style="list-style-type: none"> <li>■ First used in 1976</li> </ul>	<ul style="list-style-type: none"> <li>■ Internet voting first used in 2000 primary Phoenix, Ariz.</li> </ul>
<ul style="list-style-type: none"> <li>■ With in-precinct scanning, has lowest residuals of any mechanical method</li> <li>■ Easier than punching holes</li> <li>■ Voter can read candidates right on ballot</li> </ul>	<ul style="list-style-type: none"> <li>■ Overvotes are impossible</li> <li>■ No human errors of tallying</li> <li>■ Easy for people with physical disabilities to use</li> <li>■ Good feedback</li> </ul>	<ul style="list-style-type: none"> <li>■ Vote from home</li> <li>■ People with physical disabilities can use their own special-needs setup</li> <li>■ No human errors in tallying</li> </ul>
<ul style="list-style-type: none"> <li>■ Ballot readers are slower, harder to calibrate and more prone to jamming than card readers</li> <li>■ Bulky ballot</li> <li>■ Ballot easy to spoil</li> </ul>	<ul style="list-style-type: none"> <li>■ User interface often poor</li> <li>■ Concerns about malicious software</li> <li>■ Concerns about computer obsolescence</li> </ul>	<ul style="list-style-type: none"> <li>■ Concerns about malicious software, network problems and hackers</li> </ul>
<ul style="list-style-type: none"> <li>■ Use an in-precinct scanner to catch problems and give the voter a second chance to vote</li> <li>■ Use DRE to mark ballot</li> <li>■ "Fill in the shape" version better than "connect the arrow" version</li> </ul>	<ul style="list-style-type: none"> <li>■ Test ballots</li> <li>■ Consider closed systems</li> <li>■ Test system, including on day of election</li> </ul>	<ul style="list-style-type: none"> <li>■ Use special Web browser</li> <li>■ System on a CD</li> <li>■ New approaches to security needed, such as multiple software agents</li> </ul>

\*Residual: an undervote or an overvote †Overvote: voting for too many candidates in a race (Undervote: voting for too few candidates in a race)

quired multiple human agents watching each other for mistakes or malice. The best future schemes might include computer agents that check one another and create internal audits to validate every step of the voting process. The Secure Architecture for Voting Electronically (SAVE) at the Massachusetts Institute of Technology is a demonstration research project to explore such an approach. SAVE works by having several programs carry out the same tasks, but while using such different methods that each program would have to be breached separately to compromise the final result. The system knows to call foul when too many modules disagree.

### Audit Trails

SOME CRITICS INSIST that the best way to ameliorate such attacks is by providing a separate human-readable paper ballot. This widely promoted scheme is the voter-verified paper ballot (VVPB) suggested by Rebecca Mercuri, then at Bryn Mawr College. The voting machine prints out a receipt, and the voter can look at it after voting and assure himself that at least the paper records his intention. The receipt remains behind a clear screen so no one can tamper with it during its inspection, and it is retained by the machine. If a dispute about the electronic count arises, a recount can be conducted using the printed receipts. (It is not a good idea for the voter to have a copy, because such receipts could encourage the selling of votes.)

Although the VVPB looks quite appealing at first glance, a deeper inspection exposes some serious flaws. First, it is complicated for the voter. Elections in this country often have many races. Validating all the selections on a separate paper after the ballot has been filled out is not a simple task. Experience shows

that even when confronted with a printout that tells voters in which race they have made a mistake, few are willing to go back and correct it. Anything that takes a voter's attention away from the immediate act of casting a ballot will reduce the chances of the person voting successfully. Every extra button, every extra step, every extra decision is a source of lost votes.

The scheme is also complicated for the officials. If a voter claims fraud, what is the official to do? The voter claims she voted for Jane, but both the DRE screen and the receipt show a vote for John. Should they close the polling station? On top of this, the officials are not legally allowed to see an individual voter's ballot.

VVPB addresses only a small part of the fraud problem. The paper trails themselves could be made part of a scheme for defrauding an election if a hacker tampers with the printing software. The paper can be manipulated in all the usual ways after the election.

A better option would allow people to verify their selections

### THE AUTHOR

**TED SELKER** is the Massachusetts Institute of Technology director of the California Institute of Technology/M.I.T. voting project, which evaluates the impact of technology on the election process. A large part of his research in voting concerns inventing and testing new technology. Examples include new approaches to user interfaces and ballot design and secure electronic architectures. Selker's Context Aware Computing group at the M.I.T. Media Laboratory strives to create a world in which people's desires and intentions guide computers to help them. This work is developing environments that use sensors and artificial intelligence to form keyboardless computer scenarios.

## In the Courts and in the News

In recent months, electronic voting machines have been in the news a lot, as groups file legal actions both for and against use of the machines and new problems with elections are uncovered.

—Graham P. Collins, staff editor

**March**—In a case brought by the American Association of Disabled Persons, a federal judge in Florida orders Duval County to have at least one machine that allows the visually impaired to vote without assistance at 20 percent of its polling places. Duval County appeals, and in April the judge stays his own ruling.

**April**—In Maryland, local politicians and activists from the Campaign for Verifiable Voting file suit against the Maryland Board of Elections to block the use of the state's 16,000 direct record electronic (DRE) voting machines, which do not have printers to produce paper receipts as required by state law. The move follows reports of glitches in the March 2 primary election; some voters who demanded paper ballots were given them but later learned their votes were invalidated.

**April**—Citing security and reliability concerns and following problems in the March 2 primary election, California's secretary of state bans the use, in the November 2004 election, of more than 14,000 DREs made by Diebold, Inc. He also conditionally decertifies 28,000 other DREs, pending steps to upgrade their security. [Some counties have their systems recertified in June.] Three counties file suit to block his order. A group of disabled voters also sues to undo the order. In addition, the California secretary of state recommends that the state's attorney general look into possible civil and criminal charges against Diebold because of what he calls "fraudulent actions by Diebold." A report accuses the company of breaking state

election law by installing uncertified software on DREs in four counties and then lying about those machines.

**May**—In Florida, Representative Robert Wexler sues to block the use of Election Systems and Services voting technology in Broward and Miami-Dade counties.

**June**—The League of Women Voters, which in 2003 endorsed paperless electronic voting, drops that support. Instead it adopts a resolution to favor "secure, accurate, recountable and accessible" systems such as those with printed receipts.

**June**—The head of the Election Assistance Commission calls for tougher security measures for electronic voting by the November election.

**July**—Advocacy groups in Florida ask a Tallahassee judge to step in before the August 31 primary election and override Governor Jeb Bush's decision not to allow manual recounts in the 15 counties that have touch-screen voting machines. Also in Florida, audit records of the 2002 governor's primary and general election are reported permanently lost because of computer failures. After a few days the records are rediscovered on a disk in an adjoining room.

**September**—Nevada, in a primary election, will be the first to use DREs that print paper receipts statewide.

with recorded audio feedback. An audio transcript on tape or a CD has an integrity that is harder to compromise than a collection of paper receipts. Most current electronic voting machines can be set up to speak the choices to the voter while he looks at the visual interface. The tape can be read by a computer or listened to by people. Because misreads of paper are a major difficulty with all counting machines today, the tape can be better verified than paper receipts. An audio receipt is also preferable to a paper receipt because it is hard to change or erase the audio verifications without such alterations being noticed (think about the 18-minute gap on the Watergate tapes). Also, a small number of cassette tapes or CDs are easier to store and transport than thousands of paper receipts.

Other proposals for voter verification include recording the video image of the DRE and showing the ballot as it has been received by the central counting databases while the voter is in the booth. The advantage of these techniques is that they are passive—they do not require additional actions on the part of the voter.

Here is how voting might go using a well-designed audio record. Imagine you are voting on a computer. You like Abby Roosevelt, Independent. You press the touch-screen button for your choice. The name is highlighted, and the vote button on

one side is replaced with an unvote button on the other side. The tab on the screen for this race shows that a selection has been made. The earphones you are wearing tell you that you have voted for "Ben Jefferson" (and these words are recorded on a back-up tape).

Wait a minute! "Ben Jefferson"? You realize that you must have pressed the wrong button by mistake. You study the screen and see a prominent "cancel vote" button. You press it. "Vote for Ben Jefferson for president canceled," the computer intones onto a tape and into your ears. The screen returns to its prevote state, and this time you press more carefully and are rewarded with "Vote cast for Abby Roosevelt, Independent, for president." You go on to the Senate race.

The features just described are designed to give feedback in ways you are most adept at understanding. People are good at noticing labels moving, tabs changing, and contrast and texture changes. We have trouble doing things accurately without such feedback. The audio verification comes right at a time when the user is performing the action. Perceptual tasks (seeing movement and hearing the audio) are easier to perform than cognitive ones (reading a paper receipt and remembering all the candidates one intended to vote for). A tape or CD recording is a permanent, independent transcript of your vote.

These features are all implementable now as ballot improvements on current voting machines. Extra work would be needed to allow sight- or hearing-impaired people to verify multiple records of their ballot as well.

Some researchers are studying alternatives to DREs, in the form of Internet voting or voting using familiar devices such as the phone. Since May 2002, England has been experimenting with a number of systems intended to increase turnout. These methods include mailing in optically readable paper ballots (absentee voting), using a standard phone call and the phone's keypad, using the instant-messaging facilities on cell phones and using interactive TV that is available in English homes. Swindon Borough, for example, included more than 100,000 voters in an experiment using the Internet and telephones. A 10-digit PIN was hand-delivered to voters' homes. This PIN was used in conjunction with a password the voters had been sent separately to authorize them to vote. No fraud was detected or reported. But the effort only improved turnout by 3 percentage points (from 28 to 31 percent).

In contrast, introducing the option of absentee voting increased voter turnout by 15 percentage points—but with a downside: large-scale vote buying was reported in Manchester and Bradford. (Being able to prove whom you have voted for, such as by showing the ballot you are mailing in, enables vote buying.)

## What Must Be Done

THE UNIVERSAL ADOPTION of perfect voting machines will not be happening anytime soon. But quite independent of the specific machines used, much can and should be done simply to ensure that votes are collected and accurately counted in the U.S. We must be adamant about the following improvements:

1. We must simplify the registration system. The largest loss of votes in 2000 occurred because errors in registration databases prevented people from voting. Registration databases must be properly checked, to make sure they include all eligible people who want to be registered. We must develop national standards and technology to ensure that people can register reliably but that they do not register and vote in multiple places.
2. Local election officials must understand the operation of their equipment and test its performance thoroughly when it is delivered and before each election. DREs should be tested on election day, using dummy precincts.
3. Local election officials must teach their workers using simple procedures to run the equipment and other processes. Ballot making, marking, collecting and counting all must be carefully set up to avoid error and fraud. Many voting officials inadvertently use procedures that compromise accuracy, security and integrity of ballots by, for example, turning off precinct scanning machines that check for overvotes and inspecting and “correcting” ballots.
4. Each step in the voting process must be resistant to tamper-

ing. Collecting, counting and storing of ballots must be done with documentation of who touches everything and with clear procedures for what to do with the materials at each stage. Multiple people must oversee all critical processes.

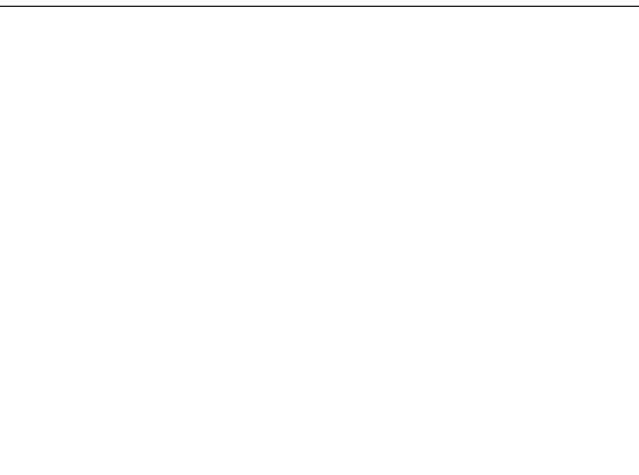
5. Each task in the voting process must be clear and accessible, have helpful feedback and allow a person to validate it. Perceptual, cognitive, motor and social capabilities of people must be taken into account when designing both machines and ballots. Ballot designs should pass usability and countability tests before being shown for final approval to the parties invested in the election.

6. The government should invest in research to develop and test secure voting technology, including DREs and Internet voting. Rushing to adopt present-day voting machines is not the best use of funds in the long term.

7. Standards of ethics must be set and enforced for all poll workers and also for voting companies regarding investments in them and donations by them or their executives.

Only when these requirements are met will we have a truly secure and accurate voting system, no matter what underlying technology is used.

SM



## MORE TO EXPLORE

**Misvotes, Undervotes and Overvotes: The 2000 Presidential Election in Florida.** Alan Agresti and Bret Presnell in *Statistical Science*, Vol. 17, No. 4, pages 436–440; 2002. Available at [web.stat.ufl.edu/~presnell/Tech-Reps/election2000.pdf](http://web.stat.ufl.edu/~presnell/Tech-Reps/election2000.pdf)

**A Better Ballot Box?** Rebecca Mercuri in *IEEE Spectrum*, Vol. 39, No. 10, pages 46–50; October 2002. Available at [www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html](http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html)

**Security Vulnerabilities and Problems with WVPT.** Ted Selker and Jon Goler. April 2004. Available at [www.vote.caltech.edu/Reports/vtp\\_wp13.pdf](http://www.vote.caltech.edu/Reports/vtp_wp13.pdf)

The Caltech/M.I.T. Voting Technology Project is at [www.vote.caltech.edu](http://www.vote.caltech.edu); the project's July 2004 report with recommendations for the 2004 presidential election is at [www.vote.caltech.edu/Reports/EAC.pdf](http://www.vote.caltech.edu/Reports/EAC.pdf)

The U.S. Election Assistance Commission Web site is at [www.eac.gov](http://www.eac.gov)