

# Right Now

The expanding Harvard universe

## BOLLIXED BALLOTS

### Voting into Vapor

FULLY ELECTRONIC SYSTEMS will record about one-third of the votes cast this November. But “Until and unless everyone understands NP-completeness and cryptographic theory,” computer-security expert Rebecca Mercuri is “adamantly opposed to the use of any fully electronic or Internet-based systems for use in anonymous balloting and vote tabulation applications.” The Radcliffe Institute fellow, a computer scientist who has studied electronic voting since 1989, believes that it is “incumbent upon all concerned with elections to refrain from procuring any system that does not provide an indisputable paper ballot which can be checked by the voter visually before deposit and used by the election board in case of a recount.”

In a 2002 article in *IEEE* [Institute of Electrical and Electronics Engineers] *Spectrum* and many more recent publications, Mercuri argues that electronic voting is problematic in three ways: computer security, auditability, and transparency. All of these, she says, may pose insoluble difficulties.

The computer-security issues stem from a class of conundrums known to logicians and computer scientists as “NP-complete.” (“NP” stands for “nondeterministic polynomial-time.”) NP-complete problems are part of complexity theory, an aspect of computer science that

deals with the resources needed to solve problems, if solving them is indeed feasible at all. Computers cannot solve NP-complete problems, except, theoretically, over an infinitely long time. Take, for example, the problem of optimizing a stock portfolio. “If computers could solve this problem, we’d all be very

wealthy!” says Mercuri, with a laugh. “But computers can only approximate an answer. The problem with voting is that we need a non-approximate answer.”

In an electronic election, an NP-complete problem arises when one asks if the computer software has been properly constructed to register and tabulate votes. “Can we prove that?” asks Mercuri. “If we could prove that computers had no viruses, then the machines could test themselves. But the fact is that computer scientists have not figured out a way to

For Rebecca Mercuri, optically scanned paper ballots are the best voting option. But if electronic balloting is required by law, she suggests the mode illustrated here. A voter in a booth uses a touch-screen display (inset, upper left) to prepare a paper ballot. She inspects and verifies the paper ballot (upper right) and deposits it into a ballot box (lower right).

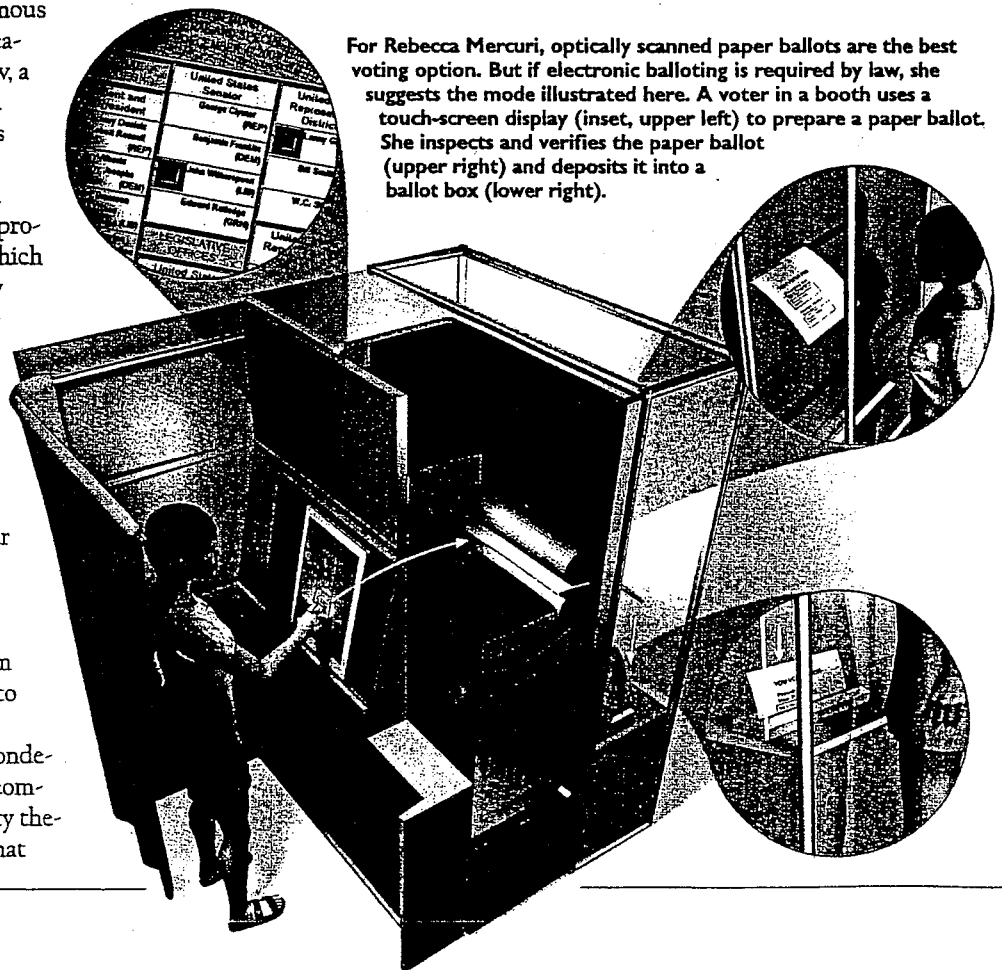


ILLUSTRATION BY BRYAN CHRISTIE

prove that the software is perfect: doing only what we want and nothing else. We *could* do it if we had infinite time and every possible input and output, but the permutations quickly become astronomical. And if you change one line of code in the software, you have to run the test again."

Voting by secret ballot also conflicts with the need for auditability. "The way we audit something like banking or healthcare precludes anonymity, since we have to track each individual transaction, end-to-end," Mercuri explains. "But anonymous voting requires privacy, so we shut off this kind of tracking during the most critical part of the process: the balloting. With this [fully electronic] equipment, you cannot perform an independent recount. It's like asking Enron to give you a printout of their accounting data." (Only one state, Nevada, requires electronic polls to be accessible to audit via voter-verified paper ballots. "Ironic, but it makes sense," Mercuri explains.

"They have to audit all these casino gaming machines, so they know how to audit computers.")

Third, says Mercuri, electronic voting "is still not sufficiently transparent for citizens of a democracy to have confidence in the system." Since computer voting involves advanced technology and complex software, "it provides an opportunity for an intellectual elite to control the system. Do you want cryptographers in control of the electoral process?"

Even so, electronic balloting is going ahead. The 2002 Help America Vote Act authorized \$3.8 billion in spending through 2006; \$3 billion of that is going to voting-systems vendors. Non-auditable, fully electronic voting technology will record 30 percent of 2004 presidential votes. Optically scanned paper ballots will tally another 50 percent, and mixed systems like lever machines and punch cards will record the remaining 20 percent. The balloting business is so con-

centrated, reports Mercuri, that two companies founded by two brothers will ultimately tabulate 80 percent of all votes cast.

"The equipment is extraordinarily expensive—small counties are paying as much as \$25 million for electronic voting machines—and frankly, unnecessary," she asserts. "These machines are only used a couple of times a year, and the rest of the time have to sit in dark, air-conditioned warehouses. Their batteries run down and need replacement. Furthermore, people are now buying obsolete machines, since the money from the Help America Vote Act wasn't tied together with technical standards. I don't see that you'll be getting much bang for your buck."

The difficulties of electronic voting reappear even more clearly in on-line Internet voting, a novelty in which France, Germany, Australia, and Estonia have announced initiatives. On-line voting poses severe problems of voter identification, as

## Right Now

well as offering vast potential for disruption by spoofing and denial-of-service attacks. "A secure Internet voting system is theoretically possible," wrote cryptographer Bruce Schneier, founder of Counterpane Internet Security, "but it would be the first secure networked application ever created in the history of computers."

Mercuri worries, too, about the

expanded scale of potential abuses.

"Whereas earlier technologies required that election fraud be perpetrated at one polling place or machine at a time," she wrote in her *IEEE Spectrum* piece, "the proliferation of similarly programmed e-voting systems invites opportunities for large-scale manipulation of elections."

She closed with a comment from an un-

named observer of voting technology:

"If you think technology can solve our voting problems," he said, "then you don't understand the problems and you don't understand the technology."

~CRAIG LAMBERT

REBECCA MERCURI WEBSITE:

[www.notablessoftware.com/evote.html](http://www.notablessoftware.com/evote.html)



REBECCA MERCURI, Ph.D.

[mercuri@acm.org](mailto:mercuri@acm.org)

215/327-7105

RADCLIFFE INSTITUTE FOR ADVANCED STUDY  
HARVARD UNIVERSITY

"All the News  
That's Fit to Print"

## Who Tests Voting Machines?

Whenever questions are raised about the reliability of electronic voting machines, election officials have a ready response: independent testing. There is nothing to worry about, they insist, because the software has been painstakingly reviewed by independent testing authorities to make sure it is accurate and honest, and then certified by state election officials. But this process is riddled with problems, including conflicts of interest and a disturbing lack of transparency. Voters should demand reform, and they should also keep demanding, as a growing number of Americans are, a voter-verified paper record of their vote.

Experts have been warning that electronic voting in its current form cannot be trusted. There is a real danger that elections could be stolen by nefarious computer code, or that accidental errors could change an election's outcome. But state officials invariably say that the machines are tested by federally selected laboratories. The League of Women Voters, in a paper dismissing calls for voter-verified paper trails, puts its faith in "the certification and standards process."

But there is, to begin with, a stunning lack of transparency surrounding this process. Voters have a right to know how voting machine testing is done. Testing companies disagree, routinely denying government officials and the public basic information. Kevin Shelley, the California secretary of state, could not get two companies testing his state's machines to answer even basic questions. One of them, Wyle Laboratories, refused to tell us anything about how it tests, or about its testers' credentials. "We don't discuss our voting machine work," said Dan Reeder, a Wyle spokesman.

Although they are called independent, these labs are selected and paid by the voting machine companies, not by the government. They can come under enormous pressure to do reviews quickly, and not to find problems, which slow things down and create additional costs. Brian Phillips, president of SysTest Labs, one of three companies that review voting machines, conceded, "There's going to be the risk of a conflict of interest when you are being paid by the vendor that you are qualifying product for."

It is difficult to determine what, precisely, the labs do. To ensure there are no flaws in the software, every line should be scrutinized, but it is hard to believe this is being done for voting software, which can contain more than a million lines. Dr. David Dill, a professor of computer science at Stanford University, calls it "basically an impossible task," and doubts it is occurring. In any case, he says, "there is no technology that can find all of the bugs and malicious things in software."

The testing authorities are currently working off 2002 standards that computer experts say are inadequate. One glaring flaw, notes Rebecca Mer-

curi, a Harvard-affiliated computer scientist, is that the standards do not require examination of any commercial, off-the-shelf software used in voting machines, even though it can contain flaws that put the integrity of the whole system in doubt. A study of Maryland's voting machines earlier this year found that they used Microsoft software that lacked critical security updates, including one to stop remote attackers from taking over the machine.

If so-called independent testing were as effective as its supporters claim, the certified software should work flawlessly. But there have been disturbing malfunctions. Software that will be used in Miami-Dade County, Fla., this year was found to have a troubling error: when it performed an audit of all of the votes cast, it failed to correctly match voting machines to their corresponding vote totals.

If independent testing were taken seriously, there would be an absolute bar on using untested and uncertified software. But when it is expedient, manufacturers and election officials toss aside the rules without telling the voters. In California, a state audit found that voters in 17 counties cast

votes last fall on machines with uncertified software. When Georgia's new voting machines were not working weeks before the 2002 election, uncertified software that was not approved by any laboratory was added to every machine in the state.

The system requires a complete overhaul. The Election Assistance Commission, a newly created federal body, has begun a review, but it has been slow to start, and it is hamstrung by inadequate finances. The commission should move rapidly to require a system that includes:

**Truly independent laboratories.** Government, not the voting machine companies, must pay for the testing and oversee it.

**Transparency.** Voters should be told how testing is being done, and the testers' qualifications.

**Rigorous standards.** These should spell out in detail how software and hardware are to be tested, and fix deficiencies computer experts have found.

**Tough penalties for violations.** Voting machine companies and election officials who try to pass off uncertified software and hardware as certified should face civil and criminal penalties.

**Mandatory backups.** Since it is extremely difficult to know that electronic voting machines will be certified and functional on Election Day, election officials should be required to have a nonelectronic system available for use.

None of these are substitutes for the best protection of all: a voter-verified paper record, either a printed receipt that voters can see (but not take with them) for touch-screen machines, or the ballot itself for optical scan machines. These create a hard record of people's votes that can be compared to the machine totals to make sure the counts are honest. It is unlikely testing and certification will ever be a complete answer to concerns about electronic voting, but they certainly are not now.



MAKING  
VOTES  
COUNT

# New Jersey Needs Auditable Voting!

## History:

- New Jersey has been gradually replacing its older voting systems with computerized ballot casting devices, known as Direct Recording Electronic (DRE) systems. Federal funding from the Help America Vote Act has accelerated this process.
- New Jersey law provides an exemption from the open bidding process for election equipment and services, so voting systems are being sold in a non-competitive “closed shop” environment. Sequoia Voting Systems has taken over the majority of the contracts, with voting systems in 11 of New Jersey’s 21 counties.

## Problems:

- DRE voting systems provide no way for voters to independently verify that their ballots have been recorded as intended, nor for the election officials to independently verify the correctness of vote totals.
- DRE voting systems have failed in actual election use, including in New Jersey, resulting in unrecoverable votes. Vendors have failed to take responsibility for their malfunctioning products, often blaming voters and election officials.
- Federal and state certification procedures are flawed, allowing blanket exemptions from examination for components that could pose critical security risks. States have discovered uncertified code in their voting systems after elections.
- Voting products that have been sold as accessible for the disabled have not worked properly. Only 8 of Mercer County’s 300 new accessible voting machines were fully functional during the 2004 spring primary election.
- DRE voting equipment contracts contain hidden costs (like software license fees), and vendors have failed to provide auditing components (such as paper ballot printers).

## Solution:

- Optically scanned paper ballots offer a cost-effective, reliable, auditable solution to elections. They are currently used by over 50% of the voters in the USA.
- These ballots can be made accessible so that disabled citizens can cast private votes.
- States have begun to adopt Accessible Voter Verified Paper Audit Trail (AVVPAT) laws that will ensure that elections using DREs are auditable and recountable.

## How You Can Help:

- Contact your county, state, and US elected officials and demand their support for verifiable voting in New Jersey. Urge them to allow the use of optically scanned paper ballots at the polling places, and encourage the passage of state laws and the development of standards requiring AVVPATs.
- If your county has DRE voting systems, consider voting by absentee ballot in November, if paper is not made available as an option.
- Read more about this – start at <<http://www.notablessoftware.com/evote.html>>.