

**SEARCH THE SITE:**
 
[Advanced Search](#)[Site Map](#)**SECTIONS:**[Front Page](#)[Today's News](#)[Information Technology](#)[Teaching](#)[Publishing](#)[Money](#)[Government & Politics](#)[Community Colleges](#)[Science](#)[Students](#)[Athletics](#)[International](#)[People](#)[Events](#)[The Chronicle Review](#)[Jobs](#)**FEATURES:**[Colloquy](#)[Colloquy Live](#)[Magazines & Journals](#)[Grants & Fellowships](#)[Facts & Figures](#)[Issues in Depth](#)[Site Sampler](#)**CHRONICLE IN PRINT:**[This Week's Issue](#)[Back Issues](#)[Related Materials](#)**SERVICES:**[About The Chronicle](#)[How to Contact Us](#)[How to Register](#)[How to Subscribe](#)[Subscriber Services](#)[Change Your User Name](#)[Change Your Password](#)[Forgot Your Password?](#)[How to Advertise](#)[Press Inquiries](#)[Corrections](#)[Privacy Policy](#)**Wary of E-Voting, Some Professors Sound the Alarm****Others say we'll byte the ballot eventually, so let's make electronic elections tamperproof**

By PETER SCHMIDT

[Easy-to-print version](#) [E-mail this article](#)

Baltimore

[Subscribe](#)

It is hard to dismiss Aviel D. Rubin as a conspiracy nut. He speaks in calm, measured tones, is an associate professor of computer science at the Johns Hopkins University, and is regarded as one of the nation's leading experts on computer security.

But the warnings that Mr. Rubin issues to the news media from his office here at the university's Information Security Institute sound as if they have been lifted from a Hollywood thriller with a trust-no-one plot.

The November 2004 presidential election could be rigged, he says. Worse yet, the public might never even know it. The culprit could be a company that manufactures electronic voting machines, or a rogue computer programmer on that company's payroll, or an election official, or a poll worker who has been bribed by foreign agents. Or someone else entirely. There's no telling just who might tamper with electronic voting machines to manipulate the democratic process.

"There are many, many, many dangers," he cautions. "And they are all independent, so none of them can be ignored."

When people are allowed to vote via the Internet -- as is becoming common in college elections -- the threats to the elections' integrity become even greater. Computer worms, viruses, and hackers at distant keyboards could wreak havoc, says Mr. Rubin.

Mr. Rubin is one of about a dozen academics around the United States, mainly computer scientists, who have been loudly warning of the risks posed by electronic voting machines and online voting. In doing so, they are also throwing wrenches into efforts to modernize the election process.

Along with grabbing headlines, these researchers are having a major impact on election policy. So far, they have dissuaded the Pentagon from trying out an online voting system for Americans living overseas. They have prompted members of Congress to introduce bills requiring that electronic voting machines spit out paper records in order to authenticate results and aid in recounts. They have persuaded six states, including California and Illinois, to adopt similar measures, and postponed the installation of electronic voting equipment by other states and municipalities.

[The Mobile Chronicle](#)  
[Help](#)

"I see a sea change," says David L. Dill, a professor of computer science at Stanford University who is also conducting research on electronic voting. "We certainly have gotten the attention of Congress, and we certainly have gotten the attention of local officials."

Even proponents of electronic voting, who feel that Mr. Rubin and Mr. Dill are crying wolf about the potential for fraud, acknowledge the critics' influence.

"They have slowed progress, for sure," says Michael I. Shamos, a professor of computer science at Carnegie Mellon University who has spent two decades evaluating electronic voting systems for state governments.

However, Mr. Shamos dismisses many of the arguments used by critics of electronic and online voting as "purely emotional" and devoid of science. "If I give them a scientific explanation of why they are wrong," he says, "they simply ignore it." He characterizes the debate as "a shrieking match," in which detractors have gained the upper hand through a slick, well-organized public-relations campaign that falsely brands demurring voices as ignorant.

"You only hear the people who are yelling," he says. "You don't hear the silent majority."

### **Early Warnings**

At the center of the debate over voting systems is a basic question: How do you conduct a fair and honest election in which each and every vote is correctly counted?

Every available technology is susceptible to glitches. Punch-card ballots can thwart the hole puncher. Scanned paper ballots can be smudged or marked too lightly. Electronic voting machines can be programmed incorrectly. Any machine used to tabulate ballots can break down.

The 2000 election debacle focused attention on these shortcomings. In response, Congress passed the Help America Vote Act of 2002, which committed \$3.9-million in federal funds to help states update election systems. Many states passed similar measures.

The cash infusion has created a surge of interest in what are technically known as "direct recording electronic" voting machines -- programmable computers that enable people to vote using touch-screens or keypads. As of the November 2000 elections, such machines were used by just over 10 percent of the electorate. By November 2002, that percentage had roughly doubled. In November 2004, nearly 29 percent of the electorate will vote on such equipment, according to Election Data Services, a Washington-based consulting firm that tracks voting and elections data.

Critics of such systems argue that officials are overlooking the threat of voting fraud in the rush to adopt such technology.

"I don't think anyone can make a sweeping statement, given the history of voting fraud, that all is well and nothing will happen," says Larry J.

Sabato, director of the Center for Politics at the University of Virginia and one of the authors of *Dirty Little Secrets: The Persistence of Corruption in American Politics* (Times Books, 1996).

Politicians "live for power -- that is their reason for getting up in the morning -- and they will do anything to maintain their power," Mr. Sabato says. Although tainted elections are less common now than they were in the 19th and early 20th centuries, he contends, there remain several states, including Illinois, Louisiana, New Jersey, and Texas, "where people are, tragically, quite tolerant of corruption" in the election process.

Election Data Services reports that come November, a substantial share of voters in Louisiana, New Jersey, and Texas are expected to cast their ballots via electronic voting machines.

### **Paper Trails**

Electronic voting machines came into being in the early 1980s, following improvements in microprocessor technology. It took nearly a decade, however, for them to attract the attention of researchers in academe. Among the first to take a hard look at such machines was Rebecca Mercuri, who is now a research fellow at Harvard University's John F. Kennedy School of Government.

In 1989 Ms. Mercuri was a doctoral student in engineering at the University of Pennsylvania and a precinct committeewoman in Lower Wakefield Township, in Pennsylvania's Bucks County. She had a master's degree in computer science, and had already worked several years as an engineer for RCA. Because her primary interests were in microsystems and in the interaction between people and computers, her ears perked up when a Bucks County commissioner said that local officials were considering the purchase of electronic voting machines.

"I just had a gut feeling that this was bad," she says, "based on what I knew about computers and consumer electronics."

Resolving to learn more about the machines, she tracked down and began working with the late Mae Churchill, a veteran voting-rights activist and leading critic of the devices. Ms. Churchill had already helped form a group called Election Watch, dedicated to publicizing the idea that the machines threatened the integrity of elections because there was no way to verify that they were working and counting ballots correctly. "She sort of roped me in," Ms. Mercuri says.

Ms. Mercuri looked to Ms. Churchill as a mentor in the realm of policy advocacy, and Ms. Churchill looked to Ms. Mercuri for technical advice about computers. Ms. Mercuri persuaded Bucks County not to buy the devices, and then Ms. Churchill pulled her into debates over voting-equipment purchases in other locations, including New York City.

In a paper presented at a 1992 conference on computer security, Ms. Mercuri proposed a fix for what she viewed as electronic voting machines' major weaknesses. She called for each machine to be equipped with a printer -- with the paper inaccessible behind glass -- to

spit out a record of how each person voted. The voter could notify precinct officials if his or her vote had been recorded incorrectly, or press a button dropping the printout into a locked ballot box if everything was OK. Election officials could retrieve the papers from the box if a recount was deemed necessary. Because the printouts would remain physically out of voters' reach, there was no risk of them walking off with the documents, and thus participating in a vote-buying scheme.

Ms. Mercuri says she never patented the proposed contraption "because I wanted it to be in the public domain." Today her approach to verifying votes, widely known as "the Mercuri method," remains the most popular idea for remedying electronic voting's perceived flaws. Advised by Ms. Mercuri, U.S. Rep. Rush Holt, a Democrat from New Jersey, introduced a bill last year calling for electronic voting machines to have such devices. The measure remains stuck in a House committee, but Sens. Hillary Clinton of New York and Bob Graham of Florida, both Democrats, recently sponsored a similar measure in the Senate.

### **Cracking the Code**

As electronic voting becomes more widespread, more researchers have become involved in the effort to shine light on the machines' inner workings and potential pitfalls.

When counties in Iowa began eyeing electronic voting machines, in 1994, state officials decided that they needed a computer expert on a state panel charged with evaluating voting equipment. They picked Douglas W. Jones, an associate professor of computer science at the University of Iowa, to fill the newly created seat, and ended up adding to the ranks of electronic-voting critics.

Early on, Mr. Jones, a computer-security expert, became convinced that the Federal Election Commission's standards for judging elections systems were too lax. He says he was surprised to find that the commission had approved voting machines with software relying on "security through obscurity" -- the notion that something is safe so long as people don't know how to get at it. In 1997 he told one manufacturer of electronic voting machines that "the moment one of the machines goes to the landfill or is otherwise disposed of, someone might extract their encryption key and all of their security claims would become meaningless."

One of the chief obstacles faced by electronic voting's critics is their inability to obtain and analyze the machines' software. For the sake of maintaining security and keeping trade secrets, the manufacturers of these machines have consistently refused to share such knowledge with any outsider unwilling to sign a nondisclosure agreement. Thus, computer scientists who *do* get a chance to examine the inner workings of the machines are precluded from discussing their findings.

In January 2003, however, Bev Harris, a writer with an interest in voting-machine security, stumbled upon the equivalent of the key under the doormat: an open Web site that employees of Diebold Election Systems, one of the nation's largest manufacturers of electronic voting machines, had used to share software code with one another.

A copy of the code used in the company's AccuVote-TS electronic voting machines found its way into the hands of Mr. Rubin of Johns Hopkins. Working with two of his doctoral students, Tadayoshi Kohno and Adam Stubblefield, and with Dan Wallach, an assistant professor of computer science at Rice University, Mr. Rubin reconstructed an electronic voting terminal in his computer lab, searching for software vulnerabilities. In a press release issued by Johns Hopkins last July, he called the system "fundamentally flawed."

Part of the group's analysis focused on the machine's reliance on "smart cards," which precinct workers give to registered voters who have presented valid identification, to insert into the machines and begin voting. They found that voters or poll workers could easily program their own smart cards and sneak them into the booth, enabling them to "cast multiple ballots without leaving any trace."

Cryptography might provide some protection from tampering, especially in the transmission of results from individual machines to the central point where votes are tallied. But the researchers concluded that "cryptography, when used at all, is used incorrectly." Both poll workers and the machines' developers had it in their power to tamper with ballots, delete or add votes, or report false results to the tallying authority.

Mr. Jones of the University of Iowa says his reading of the analysis left him outraged, because he had encountered the same problems while reviewing the software five years earlier, under a confidentiality agreement, and had warned Diebold of the need for fixes. He decided to go public with his own criticism of the machines.

Diebold hit back -- and hard. Along with issuing a 27-page report challenging the researchers' findings, the Ohio-based company accused Mr. Rubin of having a conflict of interest because he held stock in, and served on the technical advisory board of, VoteHere Inc., a developer of voting-machine software. (Mr. Rubin responded by resigning from the board, returning his stock options, and noting that he had little knowledge of, or contact with, the company, and had joined its board simply because he is friends with its chief technology officer.)

A lawyer for Diebold sent Mr. Rubin a letter declaring the software code to be the company's intellectual property and ordering him to cease and desist from using it. Lawyers for Johns Hopkins came to Mr. Rubin's aid, telling the company that he had not used the code in a way that violated the company's intellectual property rights or otherwise committed any wrongdoing, and had the university's full support.

The legal threats from Diebold ceased. And, far from backing down, Mr. Rubin, who had received media-relations training in a previous position as a computer security expert for AT&T Corporation, quickly emerged as one of the chief spokesmen for his side in the debate.

### **Science or Emotion?**

Not everyone in the field of voting research holds such a dim view of electronic voting.

Mr. Shamos of Carnegie Mellon University is one of several professors involved in the Caltech/MIT Voting Technology Project, established by the presidents of the California Institute of Technology and the Massachusetts Institute of Technology to examine voting problems in the November 2000 presidential elections. After gathering and analyzing millions of records, the group blamed most of the snafus on paper-based systems. (Remember Florida's "butterfly ballots" and "hanging chads"?)

While acknowledging that electronic voting machines have some drawbacks, the Caltech-MIT panel's members generally see such machines as a solution, rather than a threat to elections' integrity.

Britain J. Williams, a retired professor of computer science at Kennesaw State University, agrees that the criticisms have spooked election officials. "If you are an election official out there," he says, "and hear all of these respected college professors making statements about how vulnerable your computer system is, it scares you to death."

But Mr. Williams, who has spent the past 18 years evaluating computer-based voting systems for the State of Georgia, says that critics overstate the vulnerability of election systems by ignoring numerous safeguards already in place. "What they are doing," he says of critics, "is eroding the general public's confidence in our election system."

### **Unplugging Online Voting**

Among the problems examined by the Caltech-MIT panel was the difficulty that some Americans living abroad, including military personnel, encountered in trying to cast absentee ballots. The Department of Defense had considered trying out an online voting system for people abroad in the 2004 presidential election and primaries, but, thanks to Mr. Rubin and some like-minded colleagues, that experiment was nipped in the bud.

The Secure Electronic Registration and Voting Experiment, or Serve, would have allowed up to 100,000 Americans living abroad to use the Internet to register and vote in their home districts. The Defense Department had already tried a small-scale experiment involving 84 people living in the United States but residing away from the communities where they were registered to vote, in 2000. Last summer it appointed a 10-member panel of experts, 8 of them computer scientists, to examine the expansion of the proposed system.

Along with Mr. Rubin, the panel included David Wagner, an assistant professor of computer science at the University of California at Berkeley, and David R. Jefferson, a computer scientist at the Lawrence Livermore National Laboratory. (Three years earlier, Mr. Jefferson had helped convince California's secretary of state that Internet voting was too vulnerable to outside tampering to be tried.) In January they joined a fourth panel member, Barbara Simons, a technology-policy consultant, in issuing a report and press release independent of the panel alleging that the system had security vulnerabilities that could jeopardize voter privacy and allow votes to be altered.

The group raised the specter of hackers, or even terrorists, altering a close election by, for instance, creating phony Web pages that looked like voting sites. Or such miscreants might spread viruses that would monitor or modify voters' choices. Or, more simply, hackers could deny voters access to computers on election day.

"Because the danger of successful large-scale attacks is so great," the breakaway panel members wrote in their report, "we reluctantly recommend shutting down the development of Serve and not attempting anything like it in the future until both the Internet and the world's home-computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear."

Other members of the panel cried foul. One, Mr. Shamos of Carnegie Mellon, says that he had devised a way to use "test votes" to ensure the system worked correctly on election day, but that the report's four authors ignored him.

Mr. Jefferson argues that consulting other panel members might have watered down the message. "I believed that it was necessary to kill this program," he says, "and I was afraid that if we included in our discussion the other panel members whose opinions were either mixed or in opposition to ours, we would have to compromise on our recommendations or compromise on our language."

The report persuaded Deputy Defense Secretary Paul Wolfowitz to scrap the system.

R. Michael Alvarez, a professor of political science at Caltech and a member of the Caltech-MIT panel, laments that "we have lost an opportunity to gather that scientific information on how an electronic voting and registration system would have worked" for people living abroad. He says that some National Guard members stationed in Iraq are likely to be disenfranchised in the current election cycle.

In February the Michigan Democratic Party let people vote online in its presidential caucuses, apparently without a hitch.

### **Search for Solutions**

Looking ahead, few voting-technology experts foresee the use of online voting in national elections any time soon. But most see the widespread adoption of electronic voting as inevitable, and are focusing their efforts on keeping such elections honest.

Mr. Dill of Stanford has gathered more than 7,000 signatures, including at least 200 from computer-science researchers, on a petition urging that all machines be equipped with a mechanism to allow voters to ensure that their ballots are counted correctly.

Although Ms. Mercuri's proposal to have the machines print out a paper record remains the most popular solution, there are others. Edwin J. Selker, an associate professor of media and arts technology at MIT and co-director of the Caltech-MIT project, argues that voters will not bother to check a paper record of their vote, and has proposed

equipping the machines with audio devices that will let voters confirm their choices via headphone, and then store their votes on tape. Other researchers, in private industry, have suggested using cryptography to produce records that will verify votes, but cannot easily be passed off by someone involved in a vote-buying scheme.

Mr. Rubin, Mr. Jones, and Mr. Jefferson have joined several other researchers who are critical of electronic voting in seeking a National Science Foundation grant to set up a research center devoted to improving the technology.

"We need to think a lot harder before we adopt new voting technology," Mr. Dill says. "I would be very reluctant to adopt some electronic scheme unless it has been thought about very, very carefully, and a lot of people were willing to put their reputations behind it."

---

<http://chronicle.com>  
Section: Research & Publishing  
Volume 50, Issue 33, Page A18

---

[Copyright](#) © 2004 by The Chronicle of Higher Education

