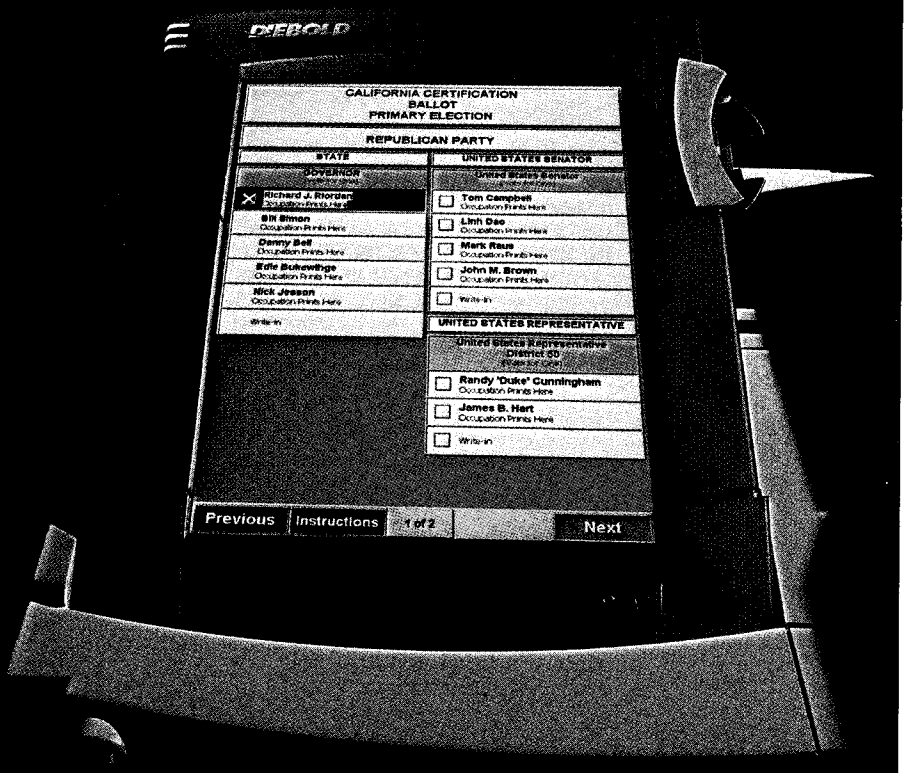
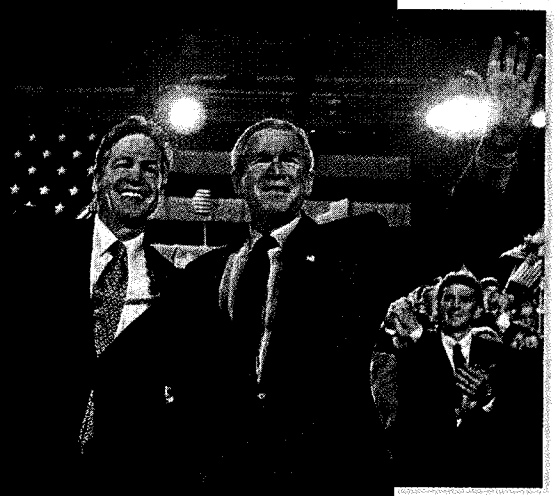


HACK THE VOTE

Glitch-prone and vulnerable to hackers, the electronic voting machines that will be in nearly every state this November could make hanging chads look benign. Outraged by the secrecy and political ties of the companies behind them, one woman has mounted a crusade against what she thinks may already be happening: untraceable election fraud

BY MICHAEL SHNAYERSON



TOUCH AND GO A Diebold touch-screen voting machine. *Inset,* then senatorial candidate Norm Coleman with President Bush in Minnesota, 2002.

INSET BY LARRY DOWNING

Florida's first election of 2004 was a small one, almost quaint. Seven Republicans were vying to fill a vacancy left by Connie Mack IV, who had resigned as state representative from Broward and Palm Beach counties to run for U.S. Congress. Everything seemed to unfold as it should, except that, of the roughly 10,000 Broward residents who signed in at the polls, 134 apparently failed to vote.

This was odd. On a ballot that listed several races, voters might skip one or another. But why go to a polling place where only one race was listed, sign in, and then not vote? For the runner-up, the question was more than academic: he lost by just 12 votes. A spokesperson for Election Systems & Software, the Nebraska-based manufacturer of the counties' new electronic voting machines, declared, "We absolutely do not believe" the machines failed to register intended votes. Perhaps 134 Democrats had wandered in to vote without realizing the slate was all-Republican, and wandered out.

Perhaps. But who knew? In the state that taught the world how to tell a dangling chad from a pregnant one, here were touch-screen voting machines that left no paper trail at all. Maybe their software had worked this time, maybe it hadn't. There was no way to tell, no back panel to open, and no way to recount.

The residents of Broward and Palm Beach counties had learned a grim new truth dawning on communities all over the country. The new generation of machine meant to save them from a reprise of Florida's 2000 debacle is a mystery box—a black box, as critics call it. Touch-screen voting machines made by four major vendors have immature technology and poor security, according to published reports. And yet by November 2, 2004, these companies, three of which have ties to wealthy Republicans, will have their machines in almost every state of the union, counting votes in the presidential election.

This is a story of good intentions gone awry, of Congress bamboozled into thinking the machines were ready when they weren't, of county and state election officials softened over lavish dinners into endorsing one kind of machine over another, with some later induced to take jobs at voting-machine companies. And

like most American stories it's about money—big money, $3.9 billion, showered on the states to buy the machines, and buy them fast.

For more than a decade, a plucky band of entrepreneurs had been tinkering with touch-screen D.R.E.'s—direct-recording electronic voting systems—that might replace various paper-ballot systems and those cumbersome lever machines. A few touch-screen D.R.E.'s had even been used in local elections. Overnight, the election chaos of 2000 made them hot commodities. Reformers and entrepreneurs pitched a future of chad-free elections, electronically perfect, and on their promises the Help America Vote Act (HAVA) was passed on October 29, 2002, with its glittering vision of an electronic voting machine in every polling place. All but ignored were the misgivings of a few computer scientists in ivory towers that the vision might be a mirage.

Harris found "a folder called 'rob-georgia,' [with] instructions to replace the files in the new Georgia voting system."

What the scientists needed was a crusader who could translate their complex software concerns into sound bites. At about the time HAVA passed into law, they got one in an unlikely package: a 52-year-old freelance writer, literary publicist, and grandmother from Seattle named Bev Harris.

Harris had been noodling online during a lunch break when she happened on an article by Lynn Landes, a freelance investigative reporter. Landes's findings about D.R.E.'s were alarming, though encrusted with arcane connections and conspiracy theories, which was perhaps why no print journalist had taken them seriously. "When it comes to elections in America," Landes typically warned, "assume crooks are in control . . . and then act accordingly."

Intrigued, Harris started sifting through the coverage of elections throughout the U.S. where D.R.E.'s had been used. She found what she thought was a disturbing pattern of Republican upsets, as well as cases in which certain brands of the machines had malfunctioned. Miscounts had always occurred, but with most D.R.E.'s there was no audit trail to set them straight. In the midterm elections of November 2002, the problem seemed to spread.

For Harris, key Senate races aroused the most suspicion. In Georgia, which in the fall of 2002 became the first state to replace all its voting machines with D.R.E.'s, a poll in the *Atlanta Journal-Constitution* put Democratic incumbent Max Cleland five points ahead of his Republican challenger, Saxby Chambliss, two days before the election. Yet Chambliss won by 7 percent: a 12-point shift in 48 hours. In Minnesota, Democrat Walter Mondale also led in two of three polls on Election Day 2002, seemingly inheriting Paul Wellstone's margin after Wellstone's fatal plane crash. Yet in a state where many votes were counted by optical-scan systems—the other main kind of electronic voting machine, in which paper ballots are read and recorded electronically—Republican Norm Coleman won by 3 percent. In Colorado, where D.R.E.'s had made significant inroads, incumbent Republican Wayne Allard was judged to be running neck and neck with Democrat Tom Strickland, yet won by a margin of 5 percent. With these outcomes the Senate majority had tipped from one party to the other, shifting all committee chairmanships, with their power to set the nation's political agenda, into Republican hands.

WHO NEEDS VOTERS?
Above, President Bush with then senatorial candidate Saxby Chambliss in Georgia, 2002. *Below,* Georgia senator Max Cleland concedes defeat, November 6, 2002. Cleland had led by 5 points in a poll; Chambliss won by 7 points—a 12-point shift in two days.

"A year ago, I'd be in my basement just saying, 'What am I looking at?'" Harris recalls. "It was really overwhelming." Harris was less likely than Landes to conjure conspiracy theories. How many conspirators, after all, would it take to rig an election on D.R.E.'s? Surely more than could keep it a secret. Still, Harris felt, the odor was rank. She looked more closely at the Cleland race in Georgia. With no newspaper willing to print her findings, she posted them on her own Web site. Computer scientists who'd gone unheard began gathering to explain how Georgia's Diebold Election Systems D.R.E.'s worked—and how they might be hacked. Soon Harris had more than an online audience: she had a grass-roots movement.

Early on, Harris did Web research on Diebold and found nothing of great interest. But she knew that, a year before, Diebold had acquired Global Election Systems (G.E.S.). When she did a Google search for "gesn," she accessed a Web site. On it, she says, was an FTP link (for File Transfer Protocol, a leading system for sharing information on the Internet) that led her to an amazing find: a trove of program files used by Diebold to make its machines do what they do. One folder, strangely enough, was called "rob-georgia."

"If you learned that a $54 million order had been placed by the state of Georgia for 22,000 new voting machines, the biggest single voting-machine purchase ever, and that these machines had been installed just prior to an election," Bev Harris recounts in her book, *Black Box Voting: Ballot-Tampering in the 21st Century* (newly published in hard copy by her own Talion press and online through Plan Nine Publishing, and on her Web site, blackboxvoting.org), "and then you saw a folder called 'rob-georgia,' looked inside, and found instructions to replace the files in the new Georgia voting system with something unknown, what would you do?"

Harris hesitated, then downloaded the program files, burned them onto seven CDs, put the CDs

TOP, BY TIM SLOAN; BOTTOM, BY JOHN BAZEMORE

in a safe-deposit box, and began to read.

In its sales pitch to the state of Georgia, Diebold had declared that its AccuVote-TS machine was designed to be not only accurate but also secure. Its audit trail would record "any attempt to create, access, or delete information." Separately, Diebold explained that independent laboratories, Wyle Laboratories, Inc., and Ciber, Inc., would test the machines and ensure that they met high federal standards. The machines would also be thoroughly tested by Diebold.

None of these claims was entirely true.

From the FTP site, Harris learned that Diebold machines put in polling places could be accessed with a "supervisor smart card." Incredibly, every one of these cards had the same password—"1111"—hard-coded into the system. Anyone with a card could conceivably tamper with vote counts, or simply stop the election when he chose. Mikko Hypponen, the Finnish computer-virus hunter of F-Secure recently profiled in *Vanity Fair* (January 2004), echoes the sentiment of Harris's online gang of computer experts: "What were they thinking?"

Worse, Harris says, one of the ways certain Diebold polling-place machines were configured to relay their votes to a central server was by wireless modem. That, says Hypponen, could make an election "potentially hackable, or disruptable, from anywhere—say, from China." The machines to be used in Georgia relayed results by a landline modem, which was better—but far from hackproof. Tallies could also be uploaded from the machines to a cartridge and physically brought to the central server. But that was the cartridge that might bear results doctored by a supervisor smart card.

Most distressing, the central server, to which polling-place results were sent, employed a database engine used by Microsoft Access. The very mention of that caused computer experts to shake their heads. "Microsoft Access is great for managing electronic records of something that would otherwise be unwieldy on paper," says Taylor Bodman, a partner at the investment bank Brown Brothers Harriman. "But you don't keep serious applications on it. It's too basic and easily hacked."

On the AccuVote central server, Harris believed, a supervisor would see votes coming in on his screen through a program called GEMS. But behind it, like a second set of books, was the database engine usable by Microsoft Access, where the vote totals were stored. With a couple of mouse clicks, Harris was able to go in through Microsoft Access, as if through a back door, change vote totals, and erase any "audit trail" of her actions. The supervisor looking at his screen on GEMS would see the new tally and have no idea it had been doctored by a hacker.

Strangely, another function allowed anyone with access to the GEMS central server to create minus votes. Why, Harris wondered, would there *ever* be cause to record negative votes in an electronic voting machine? Later, Diebold spokesman David Bear would offer this response: "Yes, negative votes can be entered into GEMS. If for some reason an election administrator determines they have a need to enter negative votes, that is for them to determine, and we do not believe the system should prevent that."

"Yes, negative votes can be entered," says Diebold's David Bear. "The system should not prevent that."

Bear took issue with other points, too. The hard-coded password had been designed as a way to avoid confusion in polling places, he noted. Using a smart card to tamper with vote results was an unrealistic scenario because poll workers and election officials would be standing by. No Diebold machines, he said, were currently configured to relay votes by wireless modem. And Harris's story of hacking into the central GEMS system through Microsoft Access was not pertinent, Bear said, because with the program files Harris had "full administrative rights" to the computer she used, which no hacker would have in an election. "Since the computer that GEMS resides on is stored in a secure location and a user must log on to that server with a valid username and password, only authorized personnel could install and/or go into Access." But, as more than one computer-science expert would reply, what if the authorized personnel were the problem?

As far as Harris could tell, this appeared to be the system that Diebold had sent to Wyle and Ciber. The two labs had agreed it met standards, all right—but standards set in 1990, the Stone Age for D.R.E. technology. And so the Georgia story disclosed a larger one: the grievous lack of any federal regulatory oversight for machines that would perform the most important public function in America.

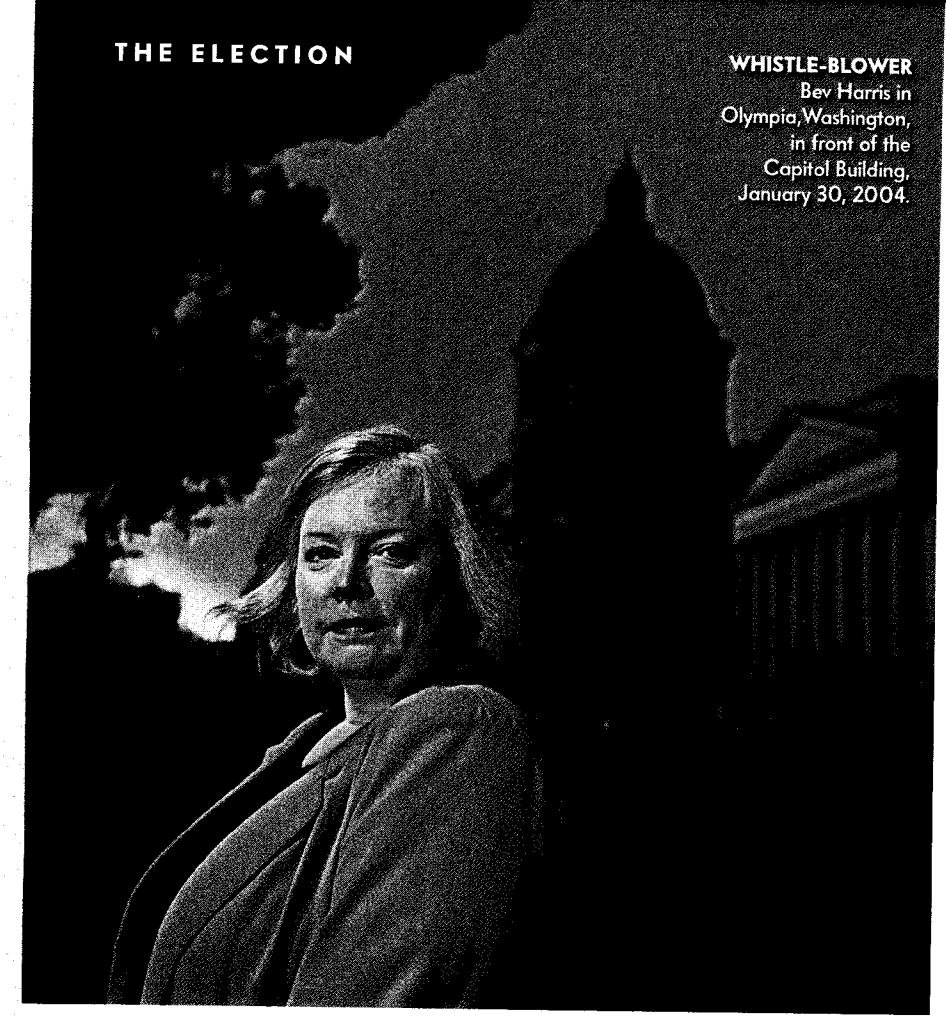
"Here's what people don't give folks credit for," grumbles Doug Lewis, head of something called the Election Center, about the 19-year effort to establish meaningful standards for voting machines. "It started in a vacuum!" Back in the mid-1980s, he explains, the states wanted standards and asked the Federal Election Commission to draw them up. The F.E.C., in turn, tried to get Congress interested. "And Congress had no interest! And now we get blamed for that!"

With no money or guidance from Congress, the job fell to the National Association of State Election Directors (NASED), which in turn tapped Lewis, down in Houston, Texas, to do a little networking from his nonprofit Election Center, which exists to "promote, preserve, and improve democracy" by working with state officials on voting issues. Lewis collaborated with Bob Naegele, an aerospace engineer in California, who had done some thinking already about standards. The manufacturers did some thinking, too. The standards wouldn't be federal, because the federal government couldn't enforce them. They would only be national in a pro forma way, because states could decide whether or not to adopt them. But they'd be a start.

And then Naegele talked to Wyle, which normally tests aerospace technology down in Huntsville, Alabama, about being the qualifying lab. It would test each kind of voting-machine system to see if it met those standards—the ones the vendors had condoned. Which Wyle proceeded to do for the whole hog—hardware and software—until the software became too onerous for it. At which point Shawn Southworth, a programmer from Huntsville, took on the software qualifying, which is pretty much exactly how Diebold's system got to Georgia.

"We did the best we could with what we had," says an aggrieved Tom Wilkey, who as director of the New York State Board of Elections pitched in as another of the standard-setters. "This program was put together without any money from anywhere, and we had to rely on the vendors. Vendors had to spend a lot of money to have their systems tested by the labs."

Bev Harris says she was unable to learn more than that about the process of qualification. The process was secret, because the systems were secret. She says that Doug Lewis, after a cursory phone talk or two, hung up on her. Wyle referred all her questions to the Election Center, which was to say Doug Lewis. So did Ciber, where Southworth worked. As for Southworth himself, he never answered a call. Harris found herself trying to get some sense of his character from Web sites, which showed pictures of him as a motorcycle enthusiast and in his office in a tight polo shirt. Doubtless he was a great guy and an excellent programmer, not to mention a fine



WHISTLE-BLOWER Bev Harris in Olympia, Washington, in front of the Capitol Building, January 30, 2004.

biker. But here was the programmer chiefly responsible for qualifying the software on all electronic voting systems in America. What if a person in a position like Southworth's found himself in dire need of money, wondered Harris. How easy would it be for one of the vendors to influence his work? And did it matter that Ciber had given $25,000 to the Republican National Committee in 2000, and in 2001 had given $23,000 to the Victory Committee for Wayne Allard?

What kind of process was this, anyway? And why was it so secret?

In the summer of 2002, the first of Diebold's D.R.E.'s arrived at a company warehouse in Georgia. Technicians began booting up the machines—the ones qualified by Wyle and Ciber and tested by Diebold. Just how many failed depends on who's telling the story.

"When we started doing acceptance testing, we began to experience a few screen freezes," acknowledges Dr. Brit Williams, professor emeritus of computer science at Georgia's Kennesaw State University, who was acting as a state evaluator of Diebold machines in this momentous experiment. "We didn't see too many . . . maybe 3½ percent failures in total. These were mostly mechanical . . . the printer didn't work, or the serial port didn't work—things like that. . . . So Diebold came to us and said they'd devised a patch to the operating system that they'd devised with Microsoft, and would we be willing to install it?"

"A year ago, I'd be in my basement just saying, 'What am I looking at?'" Harris recalls. "It was really overwhelming."

Strictly speaking, the patch should have been approved by Wyle and Ciber before it was used. But that would take months. "At that point, we looked at it internally," says Williams. "We're a computer-science department, and we have the same capability that [Wyle and Ciber] have. . . . So we put in the patch and solved the problem. As a result, all the machines worked."

Williams is a graceful southerner, well spoken, who radiates integrity. But he may not have been aware of all that was going on. "The 'rob-georgia' file contained 3,700 files of instructions to replace files that were on the machines," Harris says. "This was just one patch! There were seven other patches." According to Harris, at least two were patches for the GEMS central server. Even one patch could contain fundamental changes—for good or bad—to the system.

After Harris posted the Diebold files on her Web site in February 2003, Diebold spokesman Joseph Richardson denied that the company had put *any* patch on its 22,000 Georgia machines. "We have analyzed that situation and have no indication of that happening at all," Richardson told *Salon*'s Farhad Manjoo, one of the few reporters to pick up on the story at that time. As for the FTP site, said Richardson, it contained "old, out-of-date material."

Harris had no way of knowing, at the time, if this was true. That changed in September 2003, when someone leaked her 13,000 internal Diebold memos and e-mails. "I started reading the memos and didn't come up for air for 48 hours," Harris says. Though she remains unaware of who sent them to her, she feels their legitimacy is beyond doubt, and observes that Diebold has never disputed their contents. The memos, she believed, suggested that Diebold programmers had worked frantically through the summer and fall of 2002 to fix problems with the Georgia machines. They also appeared to make clear that the FTP site had been used that whole time, with numerous instructions and software changes posted on it to be downloaded by the technicians in Georgia. If Harris's interpretation was correct, this was a startling security gap. "The whole existence of the FTP site is just unbelievable," says F-Secure's Mikko Hypponen. Most damning, the memos seemed to reveal that a principal Diebold engineer had long been aware of the security flaws that Harris and her online gang had spotted in the FTP programs.

In one memo, that engineer, Ken Clark, freely acknowledged to a colleague that anyone could get into the central server through Microsoft Access and make changes and then erase his tracks from the audit log. Clark added that "being able to end-run the database has admittedly got people out of a bind though. Jane (I think it was Jane) did some fancy footwork on the .mdb file in Gaston recently. I know our dealers do it. King County is famous for it. That's why we've never put a password on the file before. . . . Back to perception though, if you don't bring this up [with the qualifying labs], you might skate through."

Here was a Diebold engineer admitting that the system was *not* secure. Not to mention encouraging the recipient of his memo to hide information from the labs. ("We

HAIR AND MAKEUP BY LISA DEJOHN

PHOTOGRAPH BY ROBBIE McCLARAN

don't have another version [of that story]," says Diebold's David Bear when asked about Clark's memo. "I don't know what he specifically meant.") Who was "Jane"? And what did he mean by saying that the Access back door got "people" out of a bind, and that "King County is famous for it"? Did this mean that the back door through Microsoft Access could be used to tinker with vote tallies? Harris began to wonder who was in charge at Diebold and what their political agendas were.

Diebold Election Systems is a division of the billion-dollar Diebold corporation, an Ohio-based maker of A.T.M.'s and electronic and physical security systems. Diebold Inc.'s chairman and C.E.O., Walden O'Dell, is a Bush "pioneer," having raised at least $100,000 for his re-election campaign. On June 30, 2003, he helped organize a fund-raising party that netted $600,000 and was attended by Vice President Dick Cheney. In mid-August, he sent a now infamous letter to Ohio Republicans to raise more money for the Republican Party, avowing his commitment "to helping Ohio deliver its electoral votes to the president next year."

O'Dell has since expressed regret that anyone would assume his personal politics would affect the business of Diebold Election Systems, much less the way its machines count votes. But at Diebold, politics are corporate, not just personal. In 2001 and 2002, the last years for which figures are available, Diebold Inc. gave nearly $100,000 in soft-money contributions to the Republican National Committee—and $0 to Democrats. Also, one of Diebold's directors, W. R. Timken Jr., has raised $200,000 for the Bush re-election campaign. According to *The New York Times,* 11 other Diebold executives have added a total of $22,000 to that.

None of this would matter, suggests Harvard computer scientist Rebecca Mercuri, if Diebold's software for its voting machines was open to public scrutiny. But it's not. It's a proprietary trade secret, as is that of its principal rivals. Which is why the certification process is secret as well. The irony, Mercuri adds, is that the vendors could reveal their trade secrets and still be protected by patents or copyrights—as, for example, drug companies are when they market a new drug. But that would work only if all the vendors in this fiercely competitive new industry agreed to do that: otherwise, holdouts could take unfair advantage.

O'Dell's unfortunate remarks stirred interest, at last, in mainstream newspapers that had ignored Harris's online findings for months as so much conspiracy mongering. The remarks, and Diebold's contributions, created, if nothing else, the appearance of a conflict of interest.

But if O'Dell was guilty of poor judgment, no one could accuse him of being a criminal. The same could not be said, Harris's colleague Andy Stephenson soon determined from the Diebold memos, of everyone who worked for Diebold Election Systems and the company it had purchased in 2002, Texas-based G.E.S.

One director of G.E.S., Michael K. Graye, was arrested in 1996 in Canada on tax-fraud and money-laundering charges that involved $18 million. Before he could be sentenced, he was indicted in the U.S. for stock fraud. He shuttled between prisons in New York and Ontario for 18 months, before pleading guilty in April 2003 to the tax-fraud charges in Canada.

After Graye had left G.E.S., it operated without further taint for some time. But strangely, in 2000, G.E.S. hired Jeffrey Dean as a senior vice president, according to S.E.C. filings, despite the fact that he had served time on 23 felony counts of embezzlement involving, as a court document cites, "a high degree of sophistication and planning in the use and alteration of records in the computerized accounting system that defendant maintained for the victim" in a law firm. Dean had been released from prison in Vancouver in 1995 with $87 in his inmate account, while owing $385,227 to the victim of his embezzlements. Yet he and his wife quickly became executives of Spectrum Print and Mail Services Ltd., a company that printed ballots, among other things. Spectrum was sold to G.E.S. in September 2000 for $1.6 million and stock. According to Harris's memos and e-mails, one of Dean's realms of responsibility was King County, Washington. Was it the same King County famous for "fancy footwork," according to Diebold engineer Ken Clark? Almost certainly, given that this was the only King County served by Diebold machines.

"Now, imagine," says Harris, "there's only about 20 guys in Vancouver. If [G.E.S.] wanted to clean up their act, why hire another shady character? And then his friend John Elder? At that point you've lost me."

Elder, Harris learned, is a convicted cocaine trafficker who served nearly five years in the same prison where Dean was incarcerated. Not long after Dean joined G.E.S., his fellow ex-con came aboard to oversee the printing of paper ballots and punch cards produced for several states. With Diebold's acquisition of G.E.S. in early 2002, Dean became a consultant. Diebold's David Bear notes that Dean's criminal activities pre-dated the Diebold era and that Dean is no longer a consultant. But Elder remains at Diebold as manager of the company's printed-products division. "All that's involved is printing ballots under supervision," says Bear.

As Harris was absorbing all this, one of the technicians whom Diebold had hired in Georgia during the summer of 2002 gave her a call. He had his own story of what had happened there.

As a subcontractor, says Rob Behler, he worked on the Diebold machines for around 30 days before a "difference of opinion" with the senior project manager led to his dismissal. So perhaps he was, as he says Professor Brit Williams characterizes him, a disgruntled employee. And as he gives his account to *Vanity Fair,* almost everything he says is at odds with Williams's version, starting with the talk of "one patch." (Was he the Rob of "rob-georgia?" Harris says the file predates his arrival.)

Here was a Diebold engineer admitting that the system was *not* secure.

"Very simply, Brit Williams did not work for Diebold, so he has no idea what patches Diebold did or didn't do," Behler says. "I worked for Diebold, and I didn't seek Brit's approval for anything, because I was told to avoid him, period."

Williams, Behler clarifies, was doing "acceptance testing" on the thousands of machines arriving in various Georgia counties. Behler's job was to update the machines, then boot them up and be sure they could pass that test. "And they didn't," he says. "They had stacks and stacks of machines on pallets that had failed, bombed out. I went down to the DeKalb County warehouse, one of the larger ones, with Greg Loe, who was second in command under [Diebold Election Systems president] Bob Urosevich, he and I together, because he wanted to see the machines. I had explained, 'Don't expect a lot—they're broke, man. They do crazy crap, and they don't do the same crazy crap twice.'" According to Behler, about 25 percent of the machines—not 3 to 4 percent—failed.

Behler says that at the company's direction he assembled two "SWAT" teams of five or six people each to go in vans to the various county warehouses and debug and update the machines before Williams and his team got to them. "Wherever they were headed," Behler says, "we'd

get ahead of them and thereby try to lower the failure rate to more acceptable levels."

Even with the frantic debugging and updating, Behler says, the failure rate was about 15 percent while he was there. "And here's the really scary thing: you could test the machine and it would test fine, then you'd turn it off, power it up again, and it would fail." When they couldn't fix a machine, Behler says, his SWAT team would move it out of the warehouse and into the van. "So swap that machine, swap the barcode numbers, and replace it with a machine we believed worked."

None of this frantic effort, Behler stresses, was directed at trying to manipulate the upcoming elections. "It was all hell-bent on succeeding with these machines so [Diebold] could get contracts." Even so, as a result of those changes, not one of Diebold's 22,000 patched machines in Georgia was evaluated by Wyle and Ciber, or thus qualified by NASED to be used in an election in November 2002.

"Behler was a contract employee, and his employment was severed prior to the elections, so some things he's saying occurred were at times he wasn't even around," says Diebold's David Bear. "The state was happy with the elections, and there has never been an allegation that the vote was compromised."

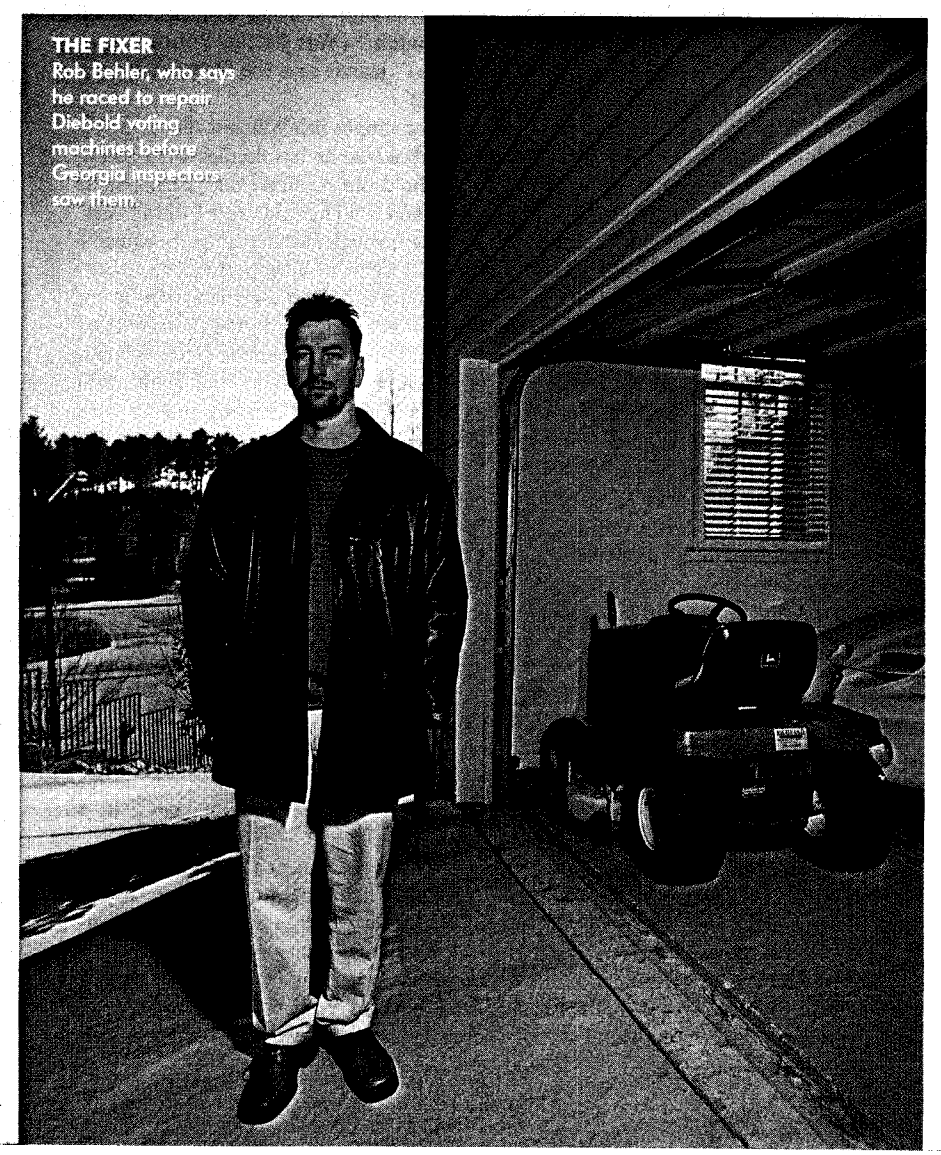
Perhaps Diebold's mad scramble to fix its machines worked. On Election Day, only a handful of them froze up, Brit Williams notes—fewer than 100, a Diebold spokesperson clarifies. And just a few other glitches were noted. Yet to Harris the outcomes seemed odd. Besides Cleland's surprise loss that November, Democratic governor Roy Barnes lost to Republican challenger Sonny Perdue: the first time in 134 years a Republican had won the governor's seat. An *Atlanta Journal-Constitution* poll had shown Barnes leading Perdue by 11 points two days before the election. "People who were inside Georgia were not surprised," says Williams. "The candidates themselves didn't challenge any of the results."

Soon after the election results were certified, Diebold wiped clean the machines used to tally those results. Williams explains that a new version of the software, incorporating "lessons learned," was installed as standard procedure. But if someone had tampered with the elections, the evidence was gone.

Diebold's Bob Urosevich bridles at the very idea that any vendor would—or could—manipulate vote results. "All the vendor does is supply a hardware which is part of a fairly big process all the way from registering voters to making voting available to the handicapped to the count and recount," he declares. "[Individuals] do not conduct elections—election officials do.

"To our knowledge," Urosevich adds, "there has not been an electronic voting system that has not recorded votes. And has not through recounts and audit logs proved to be 100 percent of what the voters' intent was."

"Wherever they were headed, we'd get ahead of them," says Behler, "and try to lower the failure rate."



THE FIXER
Rob Behler, who says he raced to repair Diebold voting machines before Georgia inspectors saw them.

PHOTOGRAPH BY ROBBIE McCLARAN

Diebold's three main rivals speak no less ardently of their own integrity, the faultless reliability and sterling security of their own touch-screen machines. But what's inside their machines remains, as in Diebold's, a lot of tightly guarded trade secrets. And so, as with Diebold, Harris had doubts and suspicions arise, fanned, with two of the three companies, by questionable ownership links.

Election Systems & Software, the Nebraska-based company whose touch-screens tallied the recent Broward–Palm Beach election in which 134 votes went unaccounted for, has grown from a tiny start-up called American Information Systems. A decade ago, the chairman of A.I.S. was Nebraskan Chuck Hagel, who stepped down from that post in 1995 to run for a U.S. Senate seat; in his surprise victory, one of the country's major upsets of 1996, many of the state's votes were counted by A.I.S. optical-scan machines. Throughout his first term, Hagel retained an indirect investment of at least $1 million in A.I.S.: his investment was in the McCarthy Group, Inc., which owned a chunk of A.I.S. Now A.I.S. has morphed into E.S.&S., but the McCarthy Group remains a minority owner of it, and Hagel still has his stake in the McCarthy Group. Chairman Michael McCarthy also served as Hagel's treasurer in his 2002 re-election campaign, raising the question: should a sen-

ator's campaign treasurer own a significant share of a private voting-machine company?

Diebold plays hard for sales, but E.S.&S. seems to play even harder. "I don't understand how with the history of performance they have—a dubious history—they can keep landing big contracts," says an executive at a rival company. "They may not be the technical choice, but they do the politics well." E.S.&S. spokesman Ken Fields replies that a survey of some 700 clients last year showed that 94 percent were "satisfied or very satisfied" with the company's equipment.

One strategy E.S.&S. has employed at least once is offering sales commissions to former election officials. In Florida, Sandra Mortham, secretary of state before the infamous Katherine Harris, was found to be accepting commissions from E.S.&S. for sales of machines statewide—a potential conflict of interest because she was also a lobbyist for the Florida Association of Counties.

"If G.E.S. wanted to clean up their act," says Harris, "why hire another shady character? And then his friend?"

Jobs, too, have been offered—and taken—though with no evidence of legal wrongdoing. In the fall of 2002, Lou Dedier, California's voting-systems director, jumped ship to manage E.S.&S.'s California operations. His government job, which involved judging whether voting systems met state standards, had made him privy to rivals' trade secrets—very useful information in his new job. *The Sacramento Bee* called on Secretary of State Bill Jones to investigate Dedier.

Jones vowed to pursue the matter, only to take a job himself last fall at Oakland, California–based Sequoia Voting Systems, now owned by England's De La Rue P.L.C. As secretary of state, Jones had sponsored a successful bond measure that raised $200 million for California counties to buy D.R.E.'s. According to the *Los Angeles Times,* the campaign was backed almost entirely with $100,000 from Sequoia and $50,000 from E.S.&S. Jones's new role, explained his communications director, Alfie Charles, to the *Times*, is "to offer counsel to election officials."

Now Charles, who not long ago sat on a panel that recommended to Jones which voting systems met state requirements, has joined Sequoia, too, as its vice president for business development. Charles still handles a lot of media inquiries, as he did in state government, so he's the one to answer an obvious question: What was Sequoia's salesman Phil Foster doing when he delivered cash-filled envelopes on five occasions to businessman Pasquale Ricci, who passed them, in turn, to Louisiana election commissioner Jerry Fowler?

Foster has never publicly explained his role in a scandal that put Fowler in jail for taking millions of dollars in kickbacks in return for having Louisiana buy voting machines and parts at inflated prices. That's because he testified before a 2001 grand jury under a grant of immunity. But Foster has a brother-in-law, J. David Philpot, who offered salient details in his guilty plea on a charge of conspiracy to commit public bribery. Philpot confirms that Foster worked for Sequoia, and that through Foster's influence Philpot was designated its "exclusive agent" for the sale of Sequoia lever voting machines in Louisiana. In fact, that designation was a sham. Philpot wanted to sell machines from his own company, Election Services Inc., and have the state buy them from him exclusively. But he had to get around a law that required the state to put out bids to all vendors. Philpot's designation as Sequoia's exclusive agent gave him the cover to do that. Fowler was happy to steer the state's lever-voting-machine business to Philpot, while appearing to comply with the Louisiana bid law, as long as Philpot was willing to pay him for the favor. This Philpot did by enlisting Foster on five occasions to put an envelope containing between $20,000 and $40,000 in the desk drawer of Pasquale Ricci, who did business with Philpot and Fowler. Fowler, in his own guilty plea, admitted retrieving the envelopes from Ricci's drawer.

"Mr. Foster never knowingly transferred cash to anybody," says his lawyer, Karl Koch. "He was never engaged in any type of criminal activity."

"The cash was not to purchase Sequoia machines, as I understand it," Charles says helpfully. "The only issues raised were whether individuals who were selling parts to Sequoia equipment were involved.... Not only was Mr. Foster not convicted, but the indictment was thrown out of court and is in the process of being expunged from the record." Indeed, Foster remains an employee at Sequoia to this day.

If both E.S.&S. and Sequoia have their little scandals, and Diebold its mess in Georgia, Hart InterCivic, fourth and corporately smallest of the major D.R.E. vendors, seems squeaky clean by comparison. Nor do any elections appear to have been thrown into disarray by Hart InterCivic machines. But the Austin, Texas–based company does have one very wealthy Republican backer, Texas investor Tom Hicks of Stratford Capital Partners

Through his main investment company, Hicks, Muse, Tate & Furst, Tom Hicks orchestrated the 1998 purchase of the Texas Rangers from George W. Bush and his partners, putting about $14.9 million into Bush's pocket. Since 1999, Hicks has personally contributed more than $125,000 to Bush and Republican causes, while investing heavily in Clear Channel Communications, the new and growing bully of the airways that dominates 238 of radio's 286 largest U.S. markets, and has a reputation for sanitizing its playlist.

"It shouldn't matter whether I'm a Democrat or Republican, because my equipment isn't Democratic or Republican," says Bill Stotesbery, Hart InterCivic's vice president of marketing. But when the equipment is secret, and the private company making it has a backer who makes six-figure political contributions, it does.

For Diebold, the Georgia experiment has led to another statewide sale, this one in Maryland, but not without withering public scrutiny.

Last July, as Maryland signed contracts to pay $55 million to Diebold, computer scientists at Johns Hopkins University declared they had pored over the Diebold program files that Bev Harris had downloaded from the company's FTP site. Lead researcher Aviel D. Rubin found what he deemed "stunning" security holes in the system.

When Doug Jones, a nationally regarded expert in computer security at the University of Iowa, read the Johns Hopkins report, he was even more surprised. He'd told Diebold to close one of the most alarming of those gaps six years before.

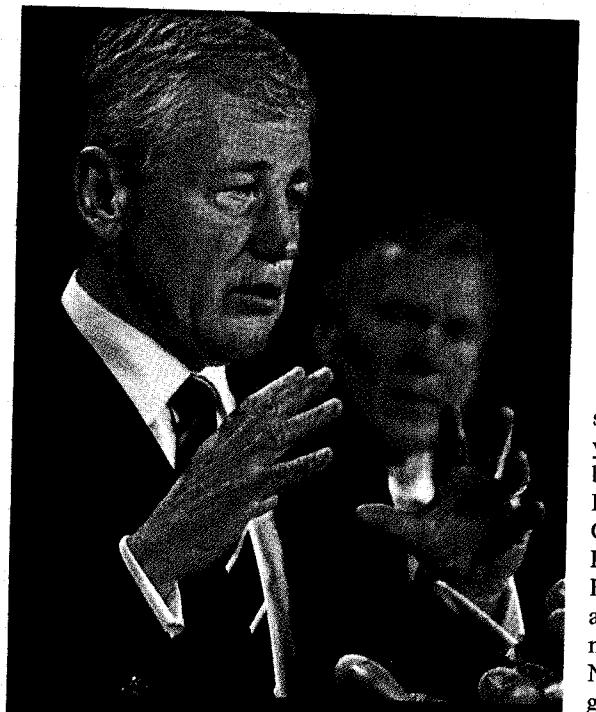
At a 1997 meeting of Iowa's board of examiners to consider D.R.E.'s, Jones recounts, he had noted with some concern that Diebold was using a federally approved encryption system called D.E.S. "Think of D.E.S. as a door-key system," Jones explains. "Everyone who wants to use my door needs a copy of the same key." That, he explains, is the issue of "key management." Other doors would need keys of their own. But not Diebold's. "Diebold was using the same key for every bit of encrypted code," he marvels. "In other words, my office-door key was being used for every door in the university!"

As Jones recalls, Bob Urosevich and other representatives of Diebold seemed confused by his line of questions. ("Per-

haps Mr. Jones didn't ask his question clearly," says Diebold's David Bear.) "Urosevich handed me his cell phone and said, 'I'm dialing my tech guy.' . . . The 'tech guy' said, 'What do you mean key management?' I said, 'You should be familiar with this term if you understand anything about cryptography: that you have to distribute keys to all users.' And he said, 'I don't think you understand—there's only one key.' At that point I was scraping my chin off the floor."

That, says Jones, is "why, when I discovered from the report that Avi Rubin et al. did that this flaw was still present, and that furthermore Diebold was defending this, I immediately called for the decertification of this system" in Iowa.

Diebold's Bear stresses that the Johns Hopkins report starts with wrong assumptions and so reaches wrong conclusions. "Rubin said he had the source code; in fact, he had a portion of the outdated code," Bear says. Moreover, he says, Rubin assumed that Diebold's polling-place machines could be hooked up to the Internet, and thus were terribly vulnerable. Wrong, says Bear: "Each touch-screen is stand-alone." Counters Rubin, "We say if these machines are connected, then these attacks are possible. If not, then that's not relevant." Bear says Rubin tested his theories in a less than real-world situation. "The election process is not just some piece of equipment," he says. "It's thousands of election officials across the country. As well as the volunteers." Bear's point is that the presence of overseers, both at the polling place and at the county seat to which precinct results are sent, creates checks and balances to any security gaps in the machines themselves. "Just because you have a good backup in place," counters Rubin, "doesn't excuse having insecure machines."



THE SOUL OF A NEW MACHINE
Nebraska senator Chuck Hagel with Tom Daschle. Hagel was chairman of A.I.S., now E.S.&S., one of the largest makers of electronic voting machines.

So far, the number of independent computer-science experts who agree with Bear appears to be zero, at least to judge by their public comments. The number of those who feel very concerned about the security of D.R.E.'s is more than 1,600. That's how many professional technologists have signed the Resolution on Electronic Voting drawn up by Stanford professor David Dill on his Web site, verifiedvoting.org. "We have the authors of the most widely read books on computer security," Dill says, "lots of experts from major universities, in addition to systems managers. At last count, we have more than 200 Ph.D. computer scientists."

After much protest from Diebold that the Johns Hopkins study was unfair because its authors had based it on the program files downloaded by Harris, the state of Maryland commissioned its own report of Diebold's system from the California-based Science Applications International Corporation (SAIC). For this one, Diebold submitted its touch-screen source code. But the study's bottom line was the same: Diebold's systems had "several high risks of vulnerabilities," which could affect the accuracy of election results.

Maryland asked Diebold to close those gaps. At the same time, to the amazement of state politicians in both parties, it announced it would go ahead with its $55 million purchase of Diebold machines.

Prodded by the resulting outcry, Maryland recently hired computer experts to try hacking into the Diebold machines. The experts succeeded with alarming ease, and went on to change vote counts both directly, on the precinct machines, and remotely, by modem. Diebold's David Bear says, "They're saying firsthand that someone can break in unnoticed, take apart the machine, turn a voter card into a supervisor's card, and change tallies. It's not a realistic scenario." He says the software issues have already been addressed.

What he doesn't say is that none would have been addressed if Bev Harris hadn't downloaded the program files that Johns Hopkins, Rubin, and others found to have such gaping security holes.

Other states are moving ahead, too. Ohio's study of all four major vendors cited the same security risks that Maryland's did, yet Ohio has told its counties to buy. So far 40 of them have chosen Diebold, 11 E.S.&S., 7 Hart InterCivic, and 4 Sequoia. In Arizona, Diebold has taken 12 counties to E.S.&S.'s 3 (although because of relative population densities E.S.&S. machines may count more votes). Nevada has shunned Diebold, but gone with Sequoia. In California, San Diego County signed on for 10,000 Diebold machines, while San Bernardino County is racing to install its Sequoia machines, and Orange County its Hart InterCivics, all before the California primary on March 2.

Amid the headlong rush, Congressman Rush Holt (Democrat, New Jersey) and Senator Hillary Clinton (Democrat, New York) have put forth bills in their respective houses of Congress to add a "paper trail" to all touch-screen machines. Every voter would receive a paper receipt of his vote, check to be sure it showed his intent, then put the receipt in a lockbox. If the number of votes at a county's various polling places failed to match the county total, a paper recount could be done. So far, 106 Democrats—and just 8 Republicans—have signed on to the House bill. But Holt will have to get his bill out of a committee ruled by Congressman Robert Ney, a Republican from Ohio—Diebold's home state.

Diebold chairman and C.E.O. Walden O'Dell is a Bush "pioneer," having raised at least $100,000 for Bush.

Regardless of what Congress does, California has now called for a paper trail on all D.R.E.'s by 2006. Why not by November 2004? That's unclear. But so, to some state election officials, are the benefits of a paper trail. "Imagine our paper ballot with 18 inches on both sides in three languages," suggests Elaine Ginnold, assistant registrar of voters for California's Alameda County. "And say it has to be absolutely secure—a paper ballot, running on a printer on D.R.E.'s, that voters can verify. And now imagine a printer jam. Or running out of toner or ink. To me

PABLO MARTINEZ MONSIVAIS

that's far worse than what we have now."

Then there's the matter of cost. Will Diebold pay for this upgrade? A clue seems to lie in one of the Diebold memos leaked to Harris, in which Ken Clark snorts at the whole debate over paper ballots being aired in the press. "There is an important point that seems to be missed by all these articles: they already bought the system. At this point they are just closing the barn door. Let's hope that as a company we are smart enough to charge out the yin if they try to change the rules now and legislate voter receipts." Asked in a subsequent memo to clarify the word "yin," Clark said he meant "out the yin-yang," meaning "any after-sale changes should be prohibitively expensive." Diebold's David Bear claims that "no one person speaks for the company. If our customers ask for paper receipts, we'll provide them."

In 2001–2002, Diebold Inc. gave nearly $100,000 in soft money to the R.N.C.—and $0 to Democrats.

Bev Harris, for one, feels a paper trail is just the start. Having paper ballots in a locked box, she notes, would solve nothing if a hacker accomplished the easy trick of having a D.R.E. tip a small percentage of one candidate's votes into the other's column without changing the total number of votes cast. Who would know that an outcome of 52–48 should have been 48–52? And so no call would come for a paper recount.

At heart, Harris says, the problem is not just a technological one, which could be solved by a better encryption code or an add-on printer for paper ballots. It's that the whole system of voting needs to be audited, like any set of books in a business—or like slot machines in a casino. "The very first thing we need to do is get solid input from auditors who are experienced in fraud detection," Harris believes. "When it comes to setting up effective auditing for these systems, bookkeepers from Las Vegas have better expertise than computer scientists from Princeton."

"Are the machines ready for prime time?" asks Dr. Brit Williams, a Georgia evaluator of D.R.E.'s. "That's a real concern, because there are deadlines: there are dates for buying machines.

"But the other thing is that elections are an ongoing process. We don't have the luxury of suspending them while we develop systems. We almost have to start with what we have and improve them from election to election." Since November 2002, Williams says, Georgia has held 300 elections on its Diebold machines. "And we've had no problems."

Or none that he knows about, given that the machines have no paper receipts.

David Dill, the Stanford computer expert militating against D.R.E.'s, says wryly that Williams is right in one sense: for a state like Georgia that's already bought its touch-screen machines, there's nothing to do but hope for the best and make incremental improvements. For any state still pondering a purchase, Dill recommends going with optical-scan machines. These, too, are electronic, but they use a paper ballot.

Former national Democratic Party chairman Joe Andrew disagrees. Andrew is something of an anomaly: a Democrat who staunchly defends touch-screen machines, and only wishes more were in place. Now a partner at a Washington law firm, he argues that, for all the problems and controversies, D.R.E.'s have a far lower error rate, overall, than any other kind of voting machine. "In the presidential election of 2000, about 7 percent of the paper ballots in Florida weren't counted correctly," he says, ticking off figures from a study published by the U.S. Commission on Civil Rights. "Optical scans had an error rate of about 6 percent, while the punch-card error rate was about 4 percent, and lever machines at 1 percent. But touch-screens in Florida had an error rate of just 0.5–1 percent. And remember, in the state that decided the election, George W. Bush won by just 537 votes out of 6 million cast."

To Andrew, the pity is that HAVA came too late to replace paper-ballot machines in significant enough numbers for the November 2004 election—and that Democrats might lose the presidential election again through voting confusions and errors created by the old system, not the new one.

Last fall, as Diebold's downloaded memos circulated ever more widely online, Diebold finally fought back. Its lawyers began issuing cease-and-desist orders to everyone who posted them, starting with Harris and including students at Swarthmore College. Swarthmore's administration removed the memos from its Web site. Then in a reversal it came to the students' legal defense. Sensing a lost cause on the field of public opinion, Diebold folded.

Now Harris plans to take Diebold to court, seeking to bar the company from selling or delivering any software that isn't properly certified. She's been a hard one to pigeonhole from the start: a journalist without training or experience, stumbling onto a national story ignored by every big-city newspaper in the land and working it deeper and deeper with scoops that would have made her career at *The New York Times* or *The Washington Post;* publishing under her own imprint because she assumed no major publisher would take her seriously; and now, because she feels more needs to be done, and pigeonholes don't matter to her, a legal activist too. "It's her character," says her daughter, Erika Hayasaki, 25, a reporter for the *Los Angeles Times.* "She's very determined and driven, so when something catches her interest, she just goes and goes and goes."

If her suit succeeds, and a broader one follows, Harris might yet keep votes from being counted on Diebold machines in the upcoming presidential election. But that's a long shot, not just for legal reasons but financial ones. Since last June, Harris has pushed aside all income-producing work to write her book. By late fall she and her husband had run through their savings and couldn't afford the $500 needed to fix a broken furnace. In her unheated home, Harris sat at her computer wrapped in an electric blanket.

Doug Lewis of the Election Center points out that a new federal agency, the Election Assistance Commission, is up and running at last, overseeing D.R.E.'s with the help of the National Institute of Standards and Technology, a division of the Commerce Department. "We don't have a darned thing to do with this stuff anymore," Lewis says with obvious relief. This is the sort of federal oversight called for by the Help America Vote Act. Unfortunately, it's come a little late for the hundreds of millions of dollars' worth of D.R.E.'s sold to counties all over the country.

With luck, perhaps, D.R.E.'s will count millions of votes in November with whirring electronic efficiency, and chads, dangling and otherwise, will be history. America will put its fears of D.R.E.'s to rest, and future elections will be tabulated as smoothly as A.T.M.'s dispense money.

That's what really worries Doug Jones.

"If I were a crook intent on stealing an election," says the Iowa expert on computer security, "I wouldn't steal it using technology which was still controversial. And I wouldn't be interested in a technology being used by only 5 percent of the voters. I would wait until that technology was being used by 65 to 80 percent of the voters and was no longer controversial, until it was so entrenched that voters felt they had no choice. That's when I'd go in and steal an election.

"And if I were competent? Without a paper trail? I'd leave no tracks." □