An open invitation to election fraud

Not only is the country's leading touch-screen voting system so badly designed that votes can be easily changed, but its manufacturer is run by a die-hard GOP donor who vowed to deliver his state for Bush next year.

By Farhad Manjoo

As if the public image of punch-card voting machines had not already been bruised and battered enough, on Sept. 15 the 9th Circuit Court of Appeals went for the K.O. Punch-card voting, a three-judge panel of the court said in its ruling halting the California gubernatorial recall election, is an embarrassment to our high-tech times: "Just as the black and white fava bean voting system of revolutionary times was replaced by paper balloting, and the paper ballot replaced by mechanical lever machine, newer technologies have emerged to replace the punch-card, including optical scanning and touch screen voting."

But according to Bev Harris, a writer who has spent more than a year investigating the shadowy world of the elections equipment industry, the replacement technologies the court cited may be worse—much worse—than the zany punch-card systems it finds so abhorrent. Specifically, Harris' research into Diebold, one of the largest providers of the new touch-screen systems, ought to give elections officials pause about mandating an all-electronic vote.

Harris has discovered that Diebold's voting software is so flawed that anyone with access to the system's computer can change the votes without leaving any record. On top of that, she's uncovered internal Diebold memos in which employees seem to suggest that the vulnerabilities are no big deal. The memos appear to be authentic—Diebold even sent Harris a notice warning her that by posting the documents on the Web, she was infringing upon the company's intellectual property. Diebold did not return several calls for comment.

The problems Harris uncovered are not all that surprising; technologists have been warning of the potential for serious flaws in electronic voting systems—especially touch-screen systems—for years. In July, scientists at Johns Hopkins and Rice found that security in Diebold's voting software fell "far below even the most minimal security standards applicable in other contexts." The report prompted Maryland Gov. Robert Ehrlich to order a review of the Diebold systems used in his state. Many of the world's most highly regarded computer scientists have called on voting companies to build touch-screen systems that print a paper ballot—a "paper trail"—in order to reduce the risk of electronic tampering.

Activists have also questioned the political affiliations of the leading voting companies. Late last year, Harris found that Sen. Chuck Hagel, a Nebraska Republican, used to run the voting company that provided most of the voting machines in his state. And in August, the Cleveland Plain Dealer reported that Walden O'Dell, the CEO of Diebold, is a major fundraiser for President Bush. In a letter to fellow Republicans, O'Dell said that he was "COMMITTED TO HELPING OHIO DELIVER ITS ELECTORAL VOTES TO THE PRESIDENT NEXT YEAR."

But the problems Harris found in Diebold's system are perhaps the best proof yet that electronic voting systems aren't ready for prime time. Indeed, the vulnerabilities in the software, as well as the internal memos, raise questions about the legitimacy of the California recall election. In its ruling, the 9th Circuit Court put the election on hold until the six counties that currently use punch-card systems—six counties that comprise 44 percent of the state's voters—upgrade their systems. On Monday, 11 judges on the 9th Circuit reheard the recall case; they may very well allow the election to go ahead on Oct. 7. If the recall vote is put on hold until March, however, many may

wonder whether to trust the results: Four of the six punch-card counties—including the largest, Los Angeles and San Diego—have plans to upgrade to Diebold machines by March. (UPDATE: On Tuesday, the appellate court ruled that the recall would go ahead as originally scheduled, on Oct. 7.)

Harris is a literary publicist and author whose investigations into the secret world of voting equipment firms have led some to call her the Erin Brockovich of elections, and who is now writing a book called "Black Box Voting." She spoke to Salon about her findings, by telephone, from her home in Seattle.

Q: Tell me about the flaw you uncovered in the Diebold system.

Well, we uncovered a few problems in the memos, but the first one that we published specifically supported the flaw that I wrote about in July of 2003. And to my surprise these memos admitted they were aware of the flaw, and it was actually brought to their attention by Ciber labs—which is a certifier—in October 2001, and they made a decision not to fix it.

Q: So it was brought to their attention two years ago?

Right.

Q: So what was the flaw?

Specifically the flaw was that you can get at the central vote-counting database through Microsoft Access. They have the security disabled. And when you get in that way, you are able to overwrite the audit log, which is supposed to log the transactions, and this [audit log] is one of the key things they cite as a security measure when they sell the system.

Q: So you can break in and then hide your tracks.

You don't even need to break in. It will open right up and in you go. You can change the votes and you can overwrite the audit trail. It doesn't keep any record of anything in the audit trail when you're in this back door, but let's say you went in the front door and you didn't want to have anything you did there appear anywhere—you can then go in the backdoor and erase what you did.

Q: Who would have access to this? Are we talking about elections officials?

A couple situations. Obviously anybody who has access to the computer, whether that's the election supervisor, their assistants, the IT people, the janitor—anybody who has access to the computer can get into it.

Q: Where is this computer—is there one per county?

Yes, there's one per county.

The other situation would be supposing someone gets in by either hacking the telephone system or by going backwards in through the Internet, because the Internet does connect to these GEMS computers, even though they deny it. A lot of the press watches election results come in on the Web and what they're watching is actually being uploaded directly off the GEMS computer.

Q: These computers in the counties are connected to the Internet, and someone can go through the Internet—

—and just go into it, correct. It would be as the results are uploading. You see, they make a big point of the fact that there's no Internet connection to the voting machine, but that's sort of parsing the issue. That's true, in the polling places there's no Internet connection, but the voting machines connect into the GEMS machine through modem. And the GEMS machine then connects to the Internet, and that's what the press watches.

Q: And somebody who knows about this can go to each one of those GEMS machines and have access to the vote and change the results?

Yes, as they're coming in.

Q: What led you to believe that there might be this flaw in the first place?

Well I work with about 22 computer programmers who have been looking at this stuff—I'm not that brilliant. Immediately when they began looking at the GEMS program they began commenting on the fact that it has no—it's something called referential integrity. And what that means is that there are many different ways that it can become vulnerable to hacking. It has to do with how one part of the database is hooked into the next part.

I got a call from one of our more brilliant computer programmers—he's got quite a few advanced degrees—and he called me on a weekend and he said, "I want you to go to your computer." And he walked me through it just like a support tech does—open this panel, click this, do this, do that. And as I'm doing this it was appalling how easy it was. Once you know the steps, a 10-year-old can rig an election. In fact it's so easy that one of our activists, Jim March in California, put together a "rig-a-vote" CD. He's been going around showing it to elections officials, and now this CD has been making its way to Congress members.

It's shocking. All you do is double-click the icon. You go backwards through the Internet to that county computer, and if you have Microsoft Access on your machine you can walk right into that election database while it's open. It's configured for multiple access at the same time. You can be in there changing things and you can change anything you want.

Q: There's nothing—no security in this?

No, in fact in the memo, [Ken Clark, an engineer at Diebold] says specifically that they decided not to put a password on it because it was proving useful. They were using the back door to do end runs around the voting program. And he named two places where they were doing this, Gaston County, N.C., and King County, Wash.

Q: Right, in the memo he says, "King county is famous for it. That's why we've never put a password on the file before." What does that mean? Why would the counties find this useful?

I have no idea what they were doing. [But] because you can change anything on the database, they could have been doing anything, whether it was nefarious or just fixing a stupid thing that they had done. The problem is this: You should set up the program so that anything you do is going to be recorded and watched and audited—it's official. There's nothing you can do that's legitimate by going into a back door that never records anything. If you need to go change some vote total because they came out wrong, that needs to be done publicly and the candidates should be aware of it. You don't do that by going into a back door.

Q: What do officials in these counties say?

Well in Gaston County it was done by a Diebold employee. [In the memo, Clark says this employee, identified only as "Jane," "did some fancy footwork on the .mdb file in Gaston recently."] I would assume that someone would need to contact Diebold. For King County, it doesn't say whether an election official did it or whether [Diebold] did it.

Q: But it is curious wording—King County is *famous* for it.

I know! Dave Ross, who has a radio show in Seattle, called King County and asked if they would like to explain it and they said no. [In an interview with Salon on Thursday, Dean Logan, King County's elections director, could not immediately say what the reference to his county in the Diebold memo could mean. Logan, who said he has just been on the job two weeks, said he would check with members of his staff and call back.]

Q: And these counties are still using Diebold systems?

They still are.

Q: Where else are Diebold systems being used?

They're in 37 states. And, by the way, this flaw that we're discussing right now affects optical-scan and touch-screen machines equally. They both come into the GEMS program.

Diebold is actually the fastest-growing voting company in the United States right now. The reason they're the fastest-growing is they tend to sell a whole state at a time. They sold to the state of Georgia, the state of Maryland, the state of Arizona. They're trying to sell the state of Ohio. They also picked very large metro areas.

Q: Georgia used Diebold's touch-screen machines in 2002, right?

Yes.

Q: And Georgia also had some wacky results, right?

They did. They had six upsets. The most famous one is Max Cleland [the Democratic senator and the incumbent]. That's because he was quite far ahead in the polls and an 11-point shift happened overnight and [Republican] Saxby Chambliss won instead. And the other upset that surprised people was Sonny Purdue, who was the first Republican governor elected in 134 years.

Q: Do you think those elections were legitimate elections?

Well, I think that it was an illegal election in that they had no idea what software was on the machines at the time. Georgia was a situation where they had changed the software not once or twice but seven or eight times so it went through so many permutations without even being examined by anyone, and nobody has any idea what the machines did. [Harris says she confirmed these preelection changes to Diebold's software in conversations with Georgia voting officials, but Diebold denies that any changes were made. In February, Joseph Richardson, a spokesman for the company, told Salon: "We have analyzed that situation and have no indication of that happening at all."]

I do find this suspicious—they have since scrubbed clean the flash memory and gotten rid of the small cards that store the results from each touch-screen machine. They've overwritten it with a whole new thing. What's amazing is you keep paper ballots for 22 months, and they're an awful lot bulkier than these credit card-size memory cards, but for some reason they felt compelled to get rid of them all. They have also overwritten all of the GEMS programs in the counting machines. They've gone through and overwritten everything in the state.

Q: OK, so we should talk about how Diebold responded to your posting these memos.

As soon . . . a few days after we posted them they sent us a cease-and-desist letter—interestingly authenticating the memos and laying claim to them, telling us that they were copyrighted. So they claimed copyright and they told us to take them off the Web.

Q: Right. By claiming copyright they're saying they own them, so that seems to indicate they are authentic memos.

Exactly.

Q: So what's your response to their copyright claim?

Well, I don't believe you can protect intent to break the law by slapping a copyright on it. And the memos that we posted show that the law has been broken. If you can protect intent to break the law, all anybody would need to do is take their bank robbery

plans and put a copyright on it, and then say nobody can look at them because they're copyrighted.

Q: Do you really think that their memos show intent to break the law?

Oh yes, yes. The Ken Clark memo is absolutely clear. It says they have been aware of these security flaws for years and they have chosen not to correct it. He says something to the effect of, find out what it will take to make this problem go away. [Referring to a voting equipment certifier, Clark tells a colleague to "find out what it is going to take to make them happy."] He says if you don't mention [a problem] you may "skate through" certification. And talking about doing "end runs" is not a good thing either.

And what's disturbing is the very same thing that these memos are talking about—overwriting the audit log—in the presentation in which they sold their machines to the state of Georgia they specifically bring up the audit log and say that no human can change it. This shows they made fraudulent claims, frankly.

There's a thing called a Qui Tam suit which citizens can file if they feel that federal money has been spent based on fraudulent claims. I haven't done it because it gives you a gag order and I refuse to be gagged even for billions of dollars, but these things are wide open for such a thing. If you go and look at the sales documents, they made one claim after the next.

Q: So because the memos show what you say is clear intent to break the law, that's why you don't think that they have a valid copyright claim.

Well, the other issue is an overriding public interest. We are told that we are to depend on these systems in 37 states and yet they are admitting that they are easy to tamper with.

Q: Are you going to respond to them?

Well, these memos are on the Web in so many locations that we took them off and put a link to someone else who put them up. So that fulfills our requirement under the law.

Q: But do you know if it's possible for you to face any—

—any retaliation? It's certainly possible that they will try retaliation, and if so I will use the full extent of the law available to me for full discovery of everything. And I think that going through discovery will become a very uncomfortable process and perhaps put some people in jail . . . Not on our side, by the way.

At this point activists are now taking these memos from various places on the Web into their state attorneys general and asking for an investigation, and since Diebold has now authenticated them it's no longer, "I found this on the Web," it's, "I found this on the Web and Diebold says they wrote them."

Q: When Diebold is put to greater scrutiny, won't the elections officials say, "We won't go with Diebold, but we'll use touch-screen systems from this company or this company?"

Well, I think that won't fly in the long run because the same illness is afflicting all of them, and that is that they are not auditable and secret. The solution is pretty simple and obvious, and that is to get properly auditable machines. A lot of the security stuff goes away—the most bulletproof system that I know anyone has come up with is one that is a touch screen but then prints a ballot that the voter verifies.

Whatever the software is doing, if you have something with a really bulletproof audit—the voter verifying the paper, and the computer tally—if those two things match, you've got a pretty good confidence level.

If Diebold, ES&S and Sequoia want to come up with a nice paper trail, voter-verified paper trail that's a touch screen, I'm supporting them. But right now they're fighting it tooth and nail.

Q: How are they fighting it?

For one thing they had a meeting on Aug. 22—the voting machine manufacturers and the Election Center [a nonprofit management division of the National Association of State Election Directors, which handles part of the voting-machine certification process] and a lobbyist. The whole purpose of this meeting was to try to get the public to figure out how to accept machines without a paper trail.

Q: How did you find out about this meeting?

Actually, this is kind of funny. My publisher found out about this. It was a teleconference and he just called in under his own name and nobody asked him where he was from, and he sat in on the whole meeting. [Harris' publisher, David Allen, posted notes on the meeting on his Web site.]

The meeting had quite a few things of concern in it. They were being told that as an industry they had to come up with $200,000 in seven days in order to come up with a P.R. campaign to whitewash their P.R. problem, as they put it.

Q: So apparently they feel they have a problem?

Yeah, they do. And in this particular meeting, one of the things they discuss is, they say, "Now we need to make sure the press never finds out this because we don't want them to know we have a problem." [According to David Allen, Harris Miller, the president of the Information Technology Association of America, said, "We just didn't want a document floating around saying the election industry is in trouble, so they decided to put together a lobbying campaign."]

Q: Was there anything discussed about addressing the problem?

Absolutely, what they want to do is not fix the problem, but they agreed to fix the perception of the problem.

Q: Did they indicate what they thought would be a problem with printing paper ballots?

No. It was a foregone conclusion that we don't want paper.

Q: But they say that they would try to convince the public that having no paper is fine?

Right.

Q: It's rather confusing why they're fighting this . . .

Yes, actually I find it a little bit suspicious frankly.

Q: What do you mean by that?

Well—it just seems like, OK, most of us who've ever run a business before, you know what the public wants. Diebold could have early on become a hero by saying, "You know what, this is a problem, but here's what we're going to do. We're going to make sure that you guys have what you want, we're going to get you this paper ballot." And instead there's this huge amount of money being expended to avoid it. It's such a simple solution—it's too much fighting over something that's so simple and that is pretty much agreed on by all of the tech experts anyway.

Q: The last thing I wanted to talk to you about is the California recall.

Hey, you Californians. What in Sam Hill are you doing?

Q: Well—as you know, the other day the 9th Circuit Court ruled that the election should be put on hold because punch-card systems are being used in six counties. Do you have any opinion on that—on whether it's a good idea to hold off on the election because of the punch-card systems? Isn't it better to have punch cards than touch screens?

Well, here's my opinion on that. First of all I don't understand why you guys are doing this election, but be that as it may. There's a study by MIT and Caltech from 2001, and it found that optical scans lose about 3 percent of the vote, punch cards lose about 4.1 percent, and touch screens lose 5.7 percent. [Harris' numbers are a bit off. The Caltech MIT study, which was one of the most thorough investigations into what went wrong in the 2000 election, analyzed "residual votes"—"uncounted, unmarked and spoiled ballots"—caused by different types of voting machines. For the presidential race, 2.5 percent of all votes cast on punch-card machines were residual votes; the rate was slightly lower, 2.3 percent, for touch-screen machines. But in gubernatorial and senatorial races, punch-card machines had a 4.7 percent error rate, while touch-screen machines had an alarming 5.9 percent error. The study's 95-page report is available here.]

If you're going from punch cards to optical-scan ballots, that is an upgrade, but if you're going from punch cards to touch screens, that makes no sense. According to the research, the one system that is currently being sold that is less accurate than a punch card is a touch screen. The court decision doesn't make a lot of sense to me. It sounds to me that, as is so typical with this, you have people who really don't understand the issues and don't understand much about how the computer programs work forming decisions based on a combination of what politicians and vendor P.R. people say.

Q: But one of the problems with optical-scan ballots is that you have to print up a lot of paper—and, you know, if this election is postponed until March, a lot of the counties are going to have huge bills because they have to print new ballots.

Oh, goodness! I hadn't thought of that. Huge, huge bills, completely wasted.

Q: So isn't that an argument for touch-screen voting?

I think the touch screens, if they had a paper trail so that we could do a proper audit, they would be my choice. The thing is if you speak Chinese, they can print something in Chinese. There would be no reason for all these combinations of ballots that folks have. It's kind of a nightmare which would be solved with the touch screens that can print.

Q: Yes, I imagine that's one of the main selling points for touch-screen machines.

I would think so. It's just that they're not auditable. I'm not opposed to it, and I think it has tremendous advantages, but it just needs to be auditable. That's a deal-breaker—it has to be auditable. And why I've been so down on Diebold is because they're the poster child for why it has to be auditable.

Farhad Manjoo is a staff writer for Salon Technology & Business.