## Electronic Voting: What You Need To Know

By William Rivers Pitt
truthout | Interview

Monday 20 October 2003

Author's Note | In July of 2003, I sat down for an extended, free-wheeling interview in Denver with three of the smartest people I have ever met. Rebecca Mercuri, Barbara Simons, and David Dill have been at the forefront of the debate surrounding the rise of electronic touch-screen voting machines in our national elections. Sufficed to say, they are three computer scientists/engineers who are as well versed on these matters as anyone you will ever meet. Scroll quickly to the bottom of this interview before reading to view their CVs.

If you are completely new to this, the issue in brief: In the aftermath of the 2000 election, Congress passed the Help America Vote Act. After much wrangling, it appears the powers that be have settled upon electronic touch-screen voting machines as the solution. There are, however, a number of serious concerns about the viability of these machines that have been raised. The matter strikes to the heart of our democracy. If the votes are not counted properly, our democracy is broken forever. More data on this is linked below, after the CVs.

Key: 'WP' is me; 'RM' is Rebecca Mercuri; 'DD' is David Dill; 'BS' is Barbara Simons. These three scientists deserve great thanks for making this complicated and important issue so clear.

---

**WP: The ideal voting technology would have five attributes: anonymity, scalability, speed, audit and accuracy. Explain the importance of these five attributes.**

BS: Voting has to be anonymous; that's how we do voting in this country. Scalability means that when you build the system, you have to be able to use it for however many people who come to vote. It might work well for a small number of people, but not work for a large number of people. Speed is pretty clear-cut; it has to be fast and convenient, so there are no long lines of people waiting to vote. Audit means you must be able to know what happened after you vote. You must be able to prove the votes.

**WP: So with 'audit,' you're talking about recounts.**

DD: The basic idea of audits in banks, for example, is that you can reconstruct the results from the original records. In voting that means being able, even if your election system fails, or if you question it, being able to figure out what the vote totals are for an individual candidate from the original records. The original records were the paper ballots.

BS: Accuracy simply means we want to be sure the votes are accurately reported and counted.

**WP: How does this Direct Recording Electronic Voting Machine (DRE's) abrogate any of these five requirements?**

BS: It doesn't necessarily abrogate all these requirements. We are particularly concerned about audit ability.

RM: But it's not just that. With these machines, two of these requirements turn out to be in provably direct conflict. You want anonymity, but you also want audit ability. The problem you have is that those two things cannot really coexist to the fullest extent. The way that we do audit ability is that we track all transactions that happen.

Say you go to a bank ATM. The entire transaction is auditable because there's a camera, you put in a card, you have a password, and so on. At the end of the day, the withdrawal record matches the amount of money that was taken out of the bank. Audit ability and anonymity are in direct conflict because with these voting machines you have to, in some sense, shut off the audit capabilities during most critical part, which is the casting of the vote. The normal audit trail that we in computer science are used to providing is every transaction. It is everything that is happening. If something happened at 4:15, say, we're involved in proving what happened at 4:15.

What we're asking for in these Direct Recording Electronic machines is to have anonymity as well as audit ability coexisting. What the vendors have provided is an elaborate scheme whereby the votes are recorded on some sort of cartridge or recording device, but they are not recorded in sequence. They actually randomize them. They are not recorded sequentially, and by virtue of not being recorded sequentially, we don't know exactly what happens in the voting process. Something could happen in the randomization process, and that's part of the issue.

**WP: It is sounding like you have to sacrifice either anonymity or audit ability, or else come up with a way to have both coexist peacefully.**

RM: That's exactly it.

BS: What we are talking about is in some sense a simpler problem, which is still not done properly, which is just making sure the vote gets accurately recorded. Even on this simpler problem, these Direct Recording Electronic machines fail, because they don't have any way to verify the votes.

DD: If you look at this auditing problem, there's an audit gap between the voter's finger on the touch screen and the record that is made inside the machine. With DRE's as they currently work, the voter cannot tell what is being recorded inside the machine. What you really need to have is a workable audit trail, when you've got this funny anonymous system, is that the voter, before they leave the voting booth, has to be able to check that their vote has been properly recorded.

There's another company that has a fancy cryptographic scheme called VoteHere. The way they explain some of what we've said is that there are two phases to voting where you want two guarantees. One of them is making sure the voter's vote is correctly recorded. The way they say it is, "Cast As Intended." The second phase is adding up all the votes from all the precincts, which they call "Counted As Cast." These fancy schemes deal with the "Counted As Cast" problem very well, and they have various ways to deal with the "Cast as Intended" problem.

The more primitive solution that is talked about - what is available now that we can do - is either use a paper ballot system like an optical scan system, where you're filling out a paper ballot and you just put that in the ballot box, and that's the voter verified audit record. Or, and this was Rebecca's idea, is to take the touch screen machines and put a printer on it - in fact, they already have printers - and it will print the ballot, and the voter can look at that to make sure it has the right stuff on it. That then goes into the ballot box.

**WP: It strikes me - and you can correct me if I'm wrong about this - but it seems like these things you are describing with the verified voting records technologies are pretty profoundly revolutionary, over and above whatever is going on with these DRE's. I've been voting for a while now. My precinct in Boston uses those old-school monster voting machines where you yank the big lever and the curtain comes across behind you in the booth, and you throw all the vote switches, and you yank the handle back. I don't have a clue if the machine recorded my vote. I get no verification. I just haul the handle, make the sign of the cross, and hope it got recorded.**

You are talking about not only making sure that the technology within these systems functions in such a way that the votes are actually recorded, but you're adding the extra layer - giving the voters verification that their vote has been counted and recorded. Given what happened in Florida, that strikes me as one of the better ideas I've heard in a very long time.

BS: I don't think it is all that revolutionary. I voted on those old handle machines when I lived in New York, and of course there was no way to verify. But there are other systems people use to vote, like optical scans, which have been around for a while. With those, you do see your vote, and you do get a piece of paper. There is no additional technology needed. In the old days, people used paper to vote. Actually, in some sense, the lever machines you use are a step backwards. They took away the ability of the voter to make sure that the vote was at least cast the way they intended.

**WP: In Massachusetts, we had an interesting little mini-scandal with these old handle machines after the 2000 election. They realized that the machines, the interior works, hadn't been cleaned in something like thirty years, and this led to substantial vote loss.**

RM: Those traditional lever machines were actually invented by Thomas Edison. They came up with those machines because there was so much vote fraud going on - ballot stuffing and so forth - but the traditional lever machine is fully mechanical. The great thing about them is that you can crack open the back and see how it works. If there is a question whether one specific machine is working correctly, you can open up and look at the gears and the odometers like they have in cars, and you see the gears connected to the levers. It is like looking into a piano - you can watch the hammer strike the string and make the tone.

The problem, and the difference between those lever machines and these new DRE's, is that the DRE's are basically using electrons. I actually have a lot more faith in the old lever machines. I can't open the DRE and look inside and see that the button I pushed on the touch screen is being recorded inside the device. It's invisible. You can see in the old machines if a lever is connecting to the wrong place, or if there was some foul play.

The other issue is that if someone were going to do some foul play and throw an election, they'd have to go around and mess up an incredible number of those old machines, one machine at a time and one lever at a time. With these DRE's, if there's some mistake in the programming - even if it is not intentional, just some bad code - it could affect all of them, the whole quantity of the DRE's. It might not just be your city. It might be your state. It might be all the DRE's in all the counties in all the states that were provided by the manufacturer who let the bad code get by them.

**WP: Explain to me what kind of non-malicious, general screw-up errors can manifest themselves in these DRE's.**

BS: Your readers will recall when our spaceship crashed into Mars because one group involved was using feet to measure things and another was using meters. That's one example, but you might say that this was not a software error. The point is that the code was written such that it didn't work.

RM: Some of these problems are very simple. The addition of a semi-colon or an equals sign in the wrong place in a line of code can completely change the programming. This would be someone who just slipped up. There are plenty of examples of this happening. In the midterm elections down in Dallas, Texas, people tried to vote on the new touch-screen machines. They found that, no matter where they touched on the Democratic side, it would vote for the Republican candidate. These people were pretty upset, and it just kept happening and happening. In Texas they have early voting, and this problem showed up in the early voting. If this had happened on Election Day, who knows what would have transpired? They might have had to shut down voting in all of Dallas.

The Democratic Party went to court over this. They had affidavits demonstrating that there were machines making this error. Ultimately it was decided that seventeen of the machines were somehow misaligned. I don't know how that could happen, but it was decided that they were misaligned, and those machines were taken out of service.

**WP: What are the names of the companies making these DRE's?**

RM: Diebold, Sequoia and ES&S. Those are the big three.

**WP: What kind of testing are these three main companies doing to ensure that the misplaced equals sign, the misplaced semi-colon, the misaligned machine, is not happening?**

DD: I've tried to find out. What kind of testing that goes on in these companies is something we don't know. They won't tell us a thing about their code or what they do to test it.

BS: Even if we could see the code, that wouldn't be sufficient. Even if we could see the code, and even if we could convince ourselves that the code was correct, we still wouldn't know that it was the code that was running on election day.

DD: That is actually a much harder technical problem than most people would think. With current hardware, it is very difficult to make sure that the program running on the machine is the program we think is running on the machine.

There is a general theme of secrecy, which is frustrating to me. I understand some of the reasons for secrecy. It is frustrating to be because claims are made about these systems, how they are designed, how they work, that frankly I don't believe. In some cases, I don't believe it because the claims they are making are impossible. I am limited in my ability to refute these impossible claims because all the data is hidden behind a veil of secrecy.

What testing do the manufacturers do? Who the hell knows? Once it gets out of the manufacturers, we are reassured by everyone about the qualification process. There is something called the NASED Qualification Process. NASED is an organization called the National Organization of State Election Directors which has affiliated with it something called the Election Center, which I believe is a private organization. The Election Center oversees the NASED qualification process. There are Independent Testing Authorities, though their level of independence is unknown. There are three of them, called SYSTEST, CYBER and WYLE. The conventional wisdom about WYLE is that they deal with hardware and firmware. Some vendors have found out the hard way that they actually deal with all of the software that goes into the voting machine. They are the ones dealing with the software that I am most concerned about.

If you go to their web pages, it says, "If you'd like to know something about us, please go to hell" in the nicest possible way. They refer you to the Election Center, which will carefully explain to you that they scrutinize every line of code. When I was on the California Task Force dealing with all this, along with another computer scientist named David Jefferson, we wanted to know what these Independent Testing Authorities (ITA's) do. They were all invited. Everybody else on the Task Force, which included some election officials at both the state and local level, and a few people of various political affiliations, wanted to know what these Test Authorities do. So we invited them to speak to us.

SYSTEST came and spoke to us. It turns out that they are one of the small ones. They don't deal with the big stuff, and they don't deal with the software inside the voting machines. The other two, which are apparently very close, are CYBER and WYLE. They refused to come visit us. They were also too busy to join us in a phone conference. Finally, out of frustration, I wrote up ten or fifteen questions and sent it to them via the Secretary of State's office. They didn't feel like answering those questions, either.

These Test Authorities use the word 'Certified' as if it were some magical holy blessing. It's been 'Certified.' Well, what does that mean? We didn't get any answers. My friend David Jefferson has been involved in internet voting and some other election-related issues for a while now. A couple of years ago, he got the right passwords to call up WYLE and ask them what they do, and he got a description. The basic description, according to David, is that they bake the machines to see if they die. The drop them to see if they break.

And then what they do is run scripts over the computer program to check for bugs. A script is just another computer program to check for superficial things. There is no human involved. They don't want functions that are too long, and they don't want functions with multiple exit points. They say 'Modules,' but they are basically talking about chunks of code. It is basically nothing more than a style-checker, like running a spell-check. The problem with running a spell-check...

**WP: ...is that you miss the homonyms.**

DD: Right. The concept of running one of these style-checkers on a program is, at the end of the day, you know the functions are short and they don't have multiple exit points. You don't have any clue if they are doing the right thing at security holes or anywhere else. After this process, there are several other steps. There is something called an 'Acceptance Test.' When the machines get delivered to either the state or county government, they power them up and put them through the paces to make sure they work. Basically, they sign a form that says they got the thing and it's not busted. Before each election, and sometimes after each election, they have something called a Logic and Accuracy Test where, to one degree or another, they will try casting some votes on the machine to make sure they come out right. That's basically all there is to it.

As a computer scientist, I know that the worst problem that could happen is that you have someone at the company, such as a programmer who knows all the details of the code, or a mysteriously overqualified janitor, who could basically insert something malicious into the code. Given the fat that they are using the 'C' programming language, we know that such an act can be concealed. They wouldn't even have to change the program. They could just change some of the results of the program. Malicious code could be concealed in ways that are practically impossible to detect by any means, and certainly wouldn't be detectable given what we understand to be the detection and inspection process.

The computer scientist who oversees elections in Georgia told us yesterday that, by Black Box Testing, this logic and accuracy testing, he could catch any malicious code. It is completely ridiculous. If you go to the Microsoft Excel spreadsheet program, and go to row 2000, column 2000 and type a specific thing, you will get something like a flight simulator. The Microsoft programmers, even though it is a firing offense, can slip this stuff into the programming code so none of the testing people can discover it. They are called 'Easter Eggs.' If you type 'Easter Eggs' into a Google.com search, you'll get instructions on how to find all these things in Microsoft software programs.

Without even knowing very much about how these systems work, computer scientists know that you can put malicious code into a program, you can change the results of an election, and it can't be detected by inspection or testing. Period.

RM: You have to give at least some credit to this computer scientist from Georgia. He at least tests these machines. Some states just take the things out of the box from the manufacturer, plug it in and run their hands over it a few times, and then send it off for the voters to use. He, at least, takes the trouble to try and test them out.

DD: Yes. This man does the best testing of anybody in the country.

**WP: That's not very comforting.**

DD: There is just no way to test for the problems we are worried about. He is doing the best job he can.

BS: We actually heard on Tuesday morning from one of these software representatives that their software, which is 100,000 lines of code, is bug-free. That is highly unlikely.

RM: If that is true, there is a way to confirm it. We have a thing we use in the United States called the "Common Criteria." The highest level under the certification process of the Common Criteria is Level 7. This means you have to have mathematical proof for every single line of your code that it all works exactly as specified. To date, no one has done that with anything but the most simplest module. The claims we heard on Tuesday are impossible. He'd have to be super-human to accomplish this. It could be done, theoretically, but it would take forever, for that length of code, to achieve Level 7 certification. It would take longer to prove it than it would to write the code.

DD: Let me be clear. I am not a security expert, and my voting expertise is what I have picked up in the last six months. My research area is formal verification, which is mathematical proofs of the correctness of things, so I can confirm what Rebecca just said.

RM: I am a security expert.

**WP: We have talked about the non-malicious errors and glitches that can take place in these DRE codes, and in the machines themselves. What kind of malicious actions could be taken by someone against these machines? What are the security gaps? What are the ways that this process could conceivably be subject to fraud?**

DD: There are insider attacks, which we know could be successful if someone chose to do that. What people worry about with PCs is not so much Microsoft hacking them, but outside people coming in over the internet with viruses or something you download. That is an outsider attack. In order to be confident about your code, about a system that is security-sensitive, you have to do a very careful analysis of the design and the software itself. It has to be done by real pros, and it is a very labor-intensive process. That has not been done, to my knowledge, with any of these voting systems. Without that kind of analysis, you can be guaranteed that there will be gaping security holes. People are just going to make mistakes, because it is too hard to do otherwise.

Without a careful security analysis, you can't know what kind of outsider attacks may be possible. Except in the case of the Johns Hopkins paper from last week, where they managed to get their hands on the code through Diebold's carelessness and lack of security. Two graduate students noticed what turned out to be severe security blunders. I don't think it is important to emphasize whether people can hack these particular machines in these particular ways, although I find the problems these grad students found to be worrying. I think the most important thing about that is that it disproves any claim that the manufacturers or the independent testing authorities are actually carefully scrutinizing this code, or for that matter, know anything about computer security. I think we have conclusively disproven that there is anything in this process that guarantees these things are secure.

BS: Diebold has claimed that the code which was downloaded is not the code running on their machines.

There is no way to verify that this is true or not. There is reason to believe that the code which was downloaded is certified.

RM: One of the other problems brought out by the Johns Hopkins report was this issue of "Smart Cards," the things you use to cast your vote. If you had this Diebold code, you could manufacture your own Smart Cards and have a pocket full of them, and maybe cast additional votes. My issue, simply, is that it is easier than that. You don't have to be an insider in the vote machine company.

At the polling places, you have the people who are making the Smart Cards. The Smart Cards are sitting there in a pile. The interesting thing about these Smart Cards is that the voter comes to the polling place, and data is put on the Cards. The idea, as the vendors have been telling us, is that the voters take that card and go to the machine, and the card only lets them vote once. Otherwise, you could vote 20 times. What happens when there are no voters in the room at the end of the day, or in the middle of the day? What if some of the other poll workers have walked away?

There is nothing to prevent a poll worker from manufacturing some more Smart Cards, sticking them into the machine, and voting several times? There is absolutely nothing to stop some corrupt poll workers from doing this. In fact, what this whole thing was trying to prevent - they say we are using DRE's because we don't want to have these problems with paper ballots, with people taking the papers out and substituting another ballot - these same crooked people who would tamper with ballots are the same people who would make a few more Smart Cards and vote extra at the end of the day.

BS: One of the things you can do, and you don't have to be all that clever to do it, is change a small percentage of votes one way. If you're really smart, you'll change an even smaller percentage of votes the other way, so it won't be obvious. If you're smarter still, you'll do this randomly. If you're smarter still, you have something called a Random Number Generator, and maybe every hundred votes you make sure is Republican, and every five hundred votes you change to Democrat. If you try to repeat this, if you run the code again on the same input, you'll get different results, because you randomly decide what to change. Because it is random, it is different each time. You will still do the changing of 100 in one column and 500 in the other, but it will be different.

RM: These are parts of the basic underpinnings of computer science, but in actual fact, the more simple things are the ones we have been able to observe. There have been precincts where vote totals for entire candidates on these machines have come up to zero. This has happened to Republicans and Democrats. There is something wrong there.

When these vendors are asked by the newspapers about this, the vendors claim those votes were never cast. The vendors say those voters chose not to vote in those positions. All of them? In every other machines, those candidates had votes. These are simple malfunctions. Once it's done, it's done, and there's no way to go back and reconstruct it.

DD: Election officials love to believe that people go into the voting booth just for show, just to convince their friends that they are going in to vote, and then they don't vote for anybody. This is how they explain missing votes.

RM: They now have a fancy word for this: "Undervoting." They believe that, in huge numbers, people go in by the hundreds of thousands and deliberately choose not to vote.

**WP: Sounds like faking an orgasm.**

(Laughter)

DD: With something as important as elections, the government and the sellers of the machines ought to have the burden of proof on them to prove to us that the machines are working correctly, and that the election results are accurate. All of democracy is founded on the idea that the loser of an election understands that they lost fair and square, that the election represents the will of the electorate, and that they have to deal with that. If you have a situation where there is any doubt about the election, you have the kind of lasting bitterness that there is from Florida in 2000, and from Georgia in 2002. If we get into elections with outcomes that people don't believe in, where the candidates challenge the honesty of the machine, people are going to feel less and less confident in the results of elections run on these machines.

BS: I want to get back to those undervotes quickly. I think it is very unlikely in major elections, when there are only one or two candidates or positions on the ballot that people would go in with the intention of not voting. But when you have a long ballot, like you get in California, and you get to the point where you have to vote for judges, and you've never heard of any of them, many people may not vote for them. That kind of undervote is frequently legitimate. It is when there are major races, races that are pretty much what the election is about, and you don't get votes. That's when you have to be suspicious.

BS: I think that most of the comments we are making about security apply to the big three companies: Diebold, Sequoia and ES&S. What we see these three companies doing is not adequate at all.

DD: I don't see the smaller companies being much better than the big three. The basic problem is that they all float down to the lowest level, because doing everything right costs more money and takes more time. They want to get the machines out as quickly and cheaply as they can get away with, while still satisfying their customers. They have a certain set of regulations they have to satisfy. They know what the independent testing authorities are going to look at, and they don't do anything they don't need to beyond that. We can pretty much count on the security of most of these machines not being good. There are a few very computer-science-oriented companies. VoteHere is the only one I can think of. They have a different attitude on security because that is their selling point.

RM: Now that there is increased interest in voter-verified systems, there are companies coming out with new systems. You can still stick with the "mark-sense" systems, the optical scan systems, the paper ballots. The problem with those is that there are many people, blind or otherwise handicapped people, who cannot use the mark-sense system. They want to be able to vote, too. They don't want to just vote at home, or vote with assistance. They want to vote on their own in the polling places, and they should be entitled to do that. That is what the Help America Vote Act has granted them. It says people with disabilities should have the same access. We believe this completely, and also believe they should have the same access to reliability.

**WP: I suppose you talked about the insider tampering, but I haven't heard you talk about the outsider, and there's a couple of them, aren't there? The judges or the poll workers. Are they able to tap in?**

DD: Let me comment about that. So what I've said about outsiders is that without a careful security analysis, we don't know. Right? We don't know enough about the machines, and you have to know about the machines, you know, and what the outsider attacks are going to be, except in the case of this Johns Hopkins paper from last week, where they managed to get their hands on the code through Diebold's carelessness.

**WP: Lack of security.**

DD: In a half an hour, two graduate students in that group had noticed what turned out to be severe security blunders. Now I don't think it's important to emphasize whether people can hack these particular machines in these particular ways, although I find the problems they found to be worrying. I think the most important thing about that is that this proves any claims that the manufacturers or the independent testing authorities are actually carefully scrutinizing this code or, for that matter, know anything about computer security. I think we've conclusively disproven that there's anything in the process that guarantees these things are secure.

BS: One quick comment. Diebold's response is that the code that was downloaded is not the code that's running on their machines; but, of course, they are not willing to let us look at the code that's running in the machines to verify whether or not that's true. And there's reason to believe that the code that was downloaded was certified.

RM: Well we believe that, though we've never really confirmed that. But we do have someone who did certification in Iowa for many years, and he saw earlier versions of the code. And he said it was the same and it had the same problems that he had told them five years ago. So we really don't know for a fact with that code, but what we can say is that one of the problems with the Diebold code that was pointed out by the Johns Hopkins Report was this business about the Smart Cards. Pretty much, if you had this code, you could manufacture your own Smart Cards and have a pocket full of them and maybe cast additional votes. But my feeling about that is that it's easier than that. And it is to your question about not having to be an insider in the voting machine company.

At the polling places, you have the people, who are making the Smart Cards. The Smart Cards are sitting there in a pile. What happens is the voter steps up, they put some electronic stuff on the Smart Card, which the idea the vendors have been telling us is that the voter can take that card, they go to the machine and it only lets them vote once. Otherwise you could keep sticking it back in and vote 20 times. Without the card you could just step up and vote 20 times. So they give them this card to enable them to do that. What happens when there's no voters in the room at the end of the day, or in the middle of the day when there's no voters in the room? And maybe some of the other poll workers have walked away?

There's nothing that prevents a poll worker from manufacturing some more Smart Cards, walking around to the machine, sticking a couple of them in, and then at the end of the day, oh, there was these three guys who didn't vote. Well, we'll just sign them in. Now you have the numbers are even. So it's a perfect attack and there's absolutely nothing that stops corrupt coworkers. And, in fact, what this whole thing was trying to prevent, these same crooked people who would want to do that would be the same crooked people who would make a few more Smart Cards, stick them in the machine and vote extra at the end of the day. I don't see why that wouldn't happen.

DD: There's sort of a hierarchy of potential security problems, and you can look at who might be the bad guy. Having the voters be the bad guys, that has its plusses and minuses. You've got a whole variety of voters you can't control, can't do background checks. They're not necessarily people you know. So it's perhaps more probable that they would be bad guys. Having them be able to fool with the machine would be especially bad. Pollworkers are somewhat the same. It's very hard to get good pollworkers, you know. You're really not going to do background checks on them. There may be stuff where pollworkers have access that voters don't have access. And there is a difference between some voter like me making some fake Smart Cards and a pollworker using their little machine to make some fakes in Smart Cards. So there's some subtle differences.

**WP: So at the end of the day, basically, when Snieder in The Denver Post today says "I have security in my office. It's not like I let any Tom, Dick and Harry into my alarmed, cameraed and locked server room said Snieder. He uses 220 Diebold optical scanners for elections in Adams County." That does not fill you with warm and cuddly comfort.**

DD: Well, first of all, I'm talking about the insider attack, which is somebody changing the code in his machines before he gets them. Secondly, you know, I'm glad that he has physical security on his machines. That's a good thing. How hard is it to bribe the night watchman or whatever you need to do? It's not that hard. On the other hand, people don't have to work that hard to find some way to subvert these machines.

DD: We talk about how lousy the security with these machines is. That's really kind of a side issue. I think it's very true and it's a big problem but it's kind of a side issue. This problem with the insider attacks, even with the best security, cannot be stopped. We'd like to improve the security, but that's not the main thing we want. The main thing we want is this audit trail on the side to double check it, so if there is a problem with the security, we can catch it.

RM: Or a malfunction.

DD: Yeah. Or a simple malfunction.

RM: Any problem, we're going to know it. At the end of the day there's going to be a box of paper ballots and if this secured properly and we're talking about not just being secured by being in a locked paper box. We can also put codes on the bottom using all the pictographic schemes so that somebody can't substitute it. It would be demonstrated that that had to be the ones that were in the box on election day. So you can't just take one out and put another one in like people thought, you know, might be going on in Florida or in places where the punch cards are in with the optical scanning ones. If we make it a better ballot box then we'll add additional code that would make sure that that paper is actually secure.

**WP: I have a multi-tiered question in which we'd cover a couple of different issues. The sort of real left wing progressive activist types are the ones who are really worried about the problems with these newly conceived voting systems, and one of the main things that bugs them is some very simple research into who the Board of Directors are for a number of these Big Three companies. That simple research reveals these Boards as being comprised of some serious hard-core conservative Republican activists. How much you might know about that? I also want to**

**get into the fact that, despite the uproar that this has caused within the ranks of the left wing, there are some very interesting groups of people who are having trouble accepting the information that you are bringing to them. I also want to talk a little bit about how this is not some sort of bipartisan, one sided partisan issue.**

DD: So the first thing is, is it a right wing conspiracy? It bothers me deeply that there are major conservative contributors running these companies. On the other hand, if you think about it, everybody has a conflict of interest. You wouldn't want your pavement company running a voting machine company because they have a real interest in who gets elected, because they're going to get pavement contracts from them. And that's true of everybody. Everybody has political opinions. Everybody has economic interests that deal with the government. So there is no way to get some sort of independent, super-objective neutral voting machine company. It's always suspect, regardless of the sterling character of people in the companies which is why you need an independent check on everything. So trust is not a good thing in election systems. The only people you should be trusting are groups of people with opposing interests, such as election observers from different political parties.

Now in terms of the political realities of this, it seems that progressives are the people who are most energetic and passionate about it . I suspect that there would be a general rule that people who have lost a lot of elections lately are inclined to be more passionate about this than people who have won a lot elections lately.

On the other hand, this is a cause that seems to have a tremendous amount of grass roots appeal. I've been probably doing more grass roots activism than any other people in this room. Unfortunately, I am an incompetent activist. But people just come to me. They read the web page and ask how they can help. They are so concerned. On the other hand, most of the opposition to what we are talking about is coming from what you would think of as progressive and good government groups. A lot of these groups have taken an official position.

They have a bunch of very pragmatic concerns about, is it going to disrupt plans to buy equipment that will be replacing equipment that they hate? Will the equipment be unreliable? Will it add expenses to things? Will people buy what they feel is inferior equipment? They have legitimate concerns. Unfortunately, they're missing a legitimate concern which is the computer reliability and security issue.

**WP: It sounds a little bit like the decision has already been made to commit to this course, and they just don't want to hear about anything that's going to disrupt that decision.**

DD: I think that's exactly right. These people have been working on this issue for a very long time. They've made bunch of deals that were very hard to hammer out. They think they've got something satisfactory and they don't want people coming in and changing the rules.

RM: Some people are also afraid, like the League of Women Voters. I believe that they are actually afraid that if people think that we have to have a piece of paper, then we shouldn't trust the computer and we shouldn't trust elections, and that makes us even more afraid. What we're saying is the opposite. If you have just the computer, then we know people are going to have questions in their minds. If, on the other hand, you have these pieces of paper and the people can see the pieces of paper and there are poll workers who can see the pieces of paper, and when we all play an active role in making sure that those are counted correctly and that the procedures are done correctly, it's all a visible and open process and we've now opened it back up to the people, so that we the people, the citizens, are the ones who are conducting the elections, not the election officials.

BS: I'd like to comment a bit on the League of Women Voters and some of these other groups. I think there's something else that's going on. The people making these decisions don't have a good technical background and I think, in some cases, they are a bit afraid of technology. They want to believe. When they are told that you can trust these systems, they initially did believe it and they want to believe it because it makes life so much easier. And these machines are so much nicer compared to the punch cards. You don't have to worry about hanging chads and they can be made very easy to use and they can figure out how to operate them because they've done ATM's. And then we come along, the sort of spoil sports, and say, wait a minute, you can't trust these machines. And people don't like that.

BS: I personally have been in battle with The League of Women Voters. I joined the League of Women Voters a few months ago over this, because I was concerned about voting. Shortly thereafter, there was a letter in The Times from the president basically saying paper ballots aren't really necessary, which got me very nervous. I wrote to her, and almost immediately thereafter a statement appeared on their website saying you don't need voter verifiable paper ballots, that paper's not a good idea, it has all these problems, blah, blah, blah. Their statement is so bad it actually has a claim about something being a way of doing security which is just a joke. I mean, you'd flunk a student for making a claim that you get security through this method of keeping the information in different parts of the machine and in different formats. That doesn't give you the security. They refused to take it off their website.

DD: My first reaction to these things was simply, it's OK to disagree with me. But go get some competent technical advice. Don't produce things that are just embarrassing. And they're not hearing it.

RM: They're saying that they are speaking to computer scientists and yes, there are some computer scientists who believe that the paper ID is not the way to go and that there are some flaws with the way that we're doing things. But those people have yet to demonstrate that any of the things that we've said are incorrect because, in fact, all the things that we say are based on computer science theory which they, of course, have to subscribe to as well. But they have their own reasons for saying that. One of the interesting things in California is that when the vendors were asked about the printers, first some of the vendors said, well, putting in printers would be expensive. Turns out, they already have printers in the machines because they print out zeroes at the beginning of the day and totals at the end of the day. So it's no more expensive. Just have a little bit more different printers to do the paper stuff.

Then they said, well, how about buying the paper? And then they had this whole issue about, oh, we're going to have to archive the paper and it's going to cost us all this paper, there'll be paper jams. Turns out, California has a law that says that you have to print out the paper afterwards. They've got to print it out anyway. That's the way they audit it. They audit it by taking the stuff that's inside the computer, that we don't really know how it got in there and whether it's correct, and they actually print it out on pieces of paper.

BS: And then they count some of it.

RM: And they count some of it. Why don't they, if they're printing it out anyway, why don't they print it out and let us see it when we vote and they're going to print it out anyway. It'll save them a lot of time. No, they want to print it out after the fact and the voters will know that theirs are the ones that are being counted.

BS: Without these voter verifiable paper ballots or some equipment, which we don't yet know how to do, there is no way to do a recount. You do a recount, you go up to the machine and say, "Dear machine, would you please tell me what the numbers are?" and the machine says back to you, "They're the same numbers I gave you before, you dummy." Right? So what does it mean to do recount?

DD: What people have done is redefine recount to mean something other than what you think it means. So I've taken to saying, there's no way to do a meaningful recount.

RM: Or an independent recount. The recount is dependent upon the vendor. You have to take the vendor cartridges, put them in the vendor machine, and they have to be read using software provided by the vendor. There's no way for me, a computer scientist, to read those cards, even if they gave me a card which they say I cannot have because it's proprietary and it's owned by the county. But even if they could give me a card and I was allowed to read it, that would be illegal because I would have to use the secret code that is allowed to read the card. This is terrible. There is no independent way to do a recount.

BS: We basically are handing over our elections to a small number of private corporations. I mean, there's something kind of scandalous about this.

DD: Somebody coined a phrase that I liked: Instead of voter verified elections we have vendor verified elections. One point is about voter confidence. There are people and I worry about this myself, that by raising these concerns will undermine voter confidence. What they really mean there is we'll undermine voter participation. Particularly on the progressive side. People understand that voter turnout has been a tremendous problem. They need to get people out to vote and they don't want them to feel that their vote doesn't count, even if they're using these touch screen machines.

I don't believe there's any reason not to vote. For example, if you want to have politicians see common sense and stop buying touch screen machines, the only way to make yourself be heard is to vote, right? I don't subscribe to the idea that there's been any election that's necessarily been stolen using touch screen machines. It's a risk for the future. I don't know what's happened in the past but I don't think there's wholesale election fraud going on at this time.

BS: But you can't prove it.

DD: But I can't prove it, which is the whole problem.

**WP: And that's the inherent risk of that possibility hanging over this whole process that really is the ultimate point.**

DD: So when people speak about voter confidence, they need to think about it in this other way: It's the voters having confidence that the results of the election are sound. It's not just a voter participation problem; it's a question of accepting the results of elections.

The second point is that what we're noticing is that the grass roots have a lot of sympathy with the position we're expressing. They understand it intuitively and they share the same fear that we have. The civil rights organizations, I think, don't necessarily have the support of their base.

BS: Like the LCCR.

DD: The Leadership Conference on Civil Rights. It's a consortium of 180 civil rights organizations.

BS: And AFL-CIO, ACLU, AARP...

DD: Many of which are huge. The NAACP, also. But many of those individual organizations have not taken a position. I have a feeling that if they went and explained it objectively to their membership that a lot of their members would say, yeah, I think we'd better do something about this problem. So I'm not sure that these progressive groups have that much support from their membership. It's more the specialists in voting rights and whatever who have been working on this particular problem.

There's one last thing that I wanted to say. I think it's a great quote and it never gets into anything I ever say and probably for good reason. Albert Einstein said, "Make everything as simple as possible but no simpler." I think we're violating that when we try to simplify elections too much with this equipment. I think it should be as simple as possible, but when you start sacrificing integrity and cutting corners in order to simplify it more than it can be simplified, you've made a serious mistake.

BS: As far as these organizations that have taken public positions against voter authenticated paper ballots, one of the interesting things that we hear is, we find the same arguments coming at us from different people. It just makes me think that there's a small number of individuals who are going around lobbying these groups before we get to them, basically, and convincing them that this paper ballot is a bad idea, that people will have trouble with it. We heard yesterday that African Americans can't deal with it, they can't deal with this stuff. They can't read the paper ballot. It's going to disenfranchise them. This guy said, this is in front of several African Americans, I was thinking, my God, this is really insulting. It's insulting.

DD: There are studies by social scientists, particularly political scientists and on voting behavior, where they can show statistically there's certain things like punch cards, and maybe central optical scan, where you send your ballots into the central office and they run it through a scanner in batch mode.

RM: 'Batch mode' means running them all together.

DD: The studies show that this has a statistically discriminatory effect. It's not explained how that happens. Maybe the African American voters or whatever minority they're looking at are voting for the first time and aren't as familiar with the ballots. They can't really explain the phenomenon. But when you come to some of the better paper-based technologies, like precinct-based ones, the data is so thin that they can't prove that there's any discriminatory effect. I think that the advantages of touch screen machines to minority groups are being vastly overstated. At least there isn't strong evidence for it.

RM: I think that it's very, very important for people to start lobbying. If they're concerned about this, they must start lobbying all these groups. Rush holt, my congressman in New Jersey, has a bill in Congress on this. People need to get their Congressman to endorse that bill and make sure it also gets a compromise bill in the Senate and gets pushed through. We need to have these things being pushed through.

BS: I completely agree with everything Rebecca just said. What happens in 20 years when there's a major crisis? What worries me is in 20 years or less, there'll be an election where people will believe that something wrong was done and they won't be able to prove it. They will not be able to prove it and that gets back to the whole notion about competence that David was talking about before, the feeling that some of these progressive organizations are opposed to what we're pushing because they're afraid that we are raising doubts in the voters' minds. I think nothing will raise doubts in the voters' minds more than an election which they feel has been stolen by these machines and there's not a damned thing they can do. I mean, even in Florida, you could see what was going on. You can't see what's going on when these machines are counted.

When we talk about dealing with minorities or people with disabilities and talk about problems with these machines, it's all well and good to make sure that someone gets to vote. You know, people are concerned. They don't want these long lines, they don't want to make it too hard. I want to be able to vote. But you know, there's no point in your voting if your vote ain't going to be counted. Or it's not going to be recorded right. So it makes no sense to focus on voting if you don't know what's going to happen to your vote.

DD: I don't feel bad about raising the alarm. I think we have a moral obligation to tell the truth and I don't think that someone else could say that if somebody sees a serious problem they should be quiet about it so people won't worry. I mean, people have to worry or else, obviously, the problem's not going to get fixed. It's been going on too long and people like Rebecca have been complaining about it too long to believe that suddenly it's just going to get fixed unless we raise a real fuss.

**WP: Tell me about House Resolution 2239.**

RM: Well, Rush holt is my Congressman and he's actually a physicist. He was at Princeton, PhD. in physics before he went to Congress and his bill is really an important one because he's raising four points which people have completely misinterpreted. They think that by having voter verified ballots we're going to make it longer before the disabled will be able to vote. His bill actually says, we want verified ballots. They need to be required, but he also accelerates the time in which the disabled are going to get the new machines. He wants to push that forward, sooner, not later. That is an important reason for his bill.

Also in his bill is that he wants the code to be opened. He says there should be no secret code. Of course, the vendors can protect their stuff with copyrights and patents. That way, if somebody tries to copy their code and sell it in their machine, they can sue them just like anybody else. But that the voters and the people need to have the ability to actually see the code and be able to verify that and I'll get back to that in another second.

The last part of it is that he's concerned about these modems, these telecommunications devices, because they're saying that they can use those devices to send the data at the end of election date to the main precincts. If those are connected up to phones it can come in. He does not believe that there should be any especially wireless communications where anybody could be sending in packets.

Getting back to point number three, the business about verifying the code and being able to do that. Unfortunately we have a new trend in this country that was started in 2000. If you protest an election and you want a recount, you're now called a sore loser and it's unfortunate but it is your legal right. If you're a candidate you have the legal right to ask for a recount if you have very strong reason to believe, and you have to demonstrate this, reason to believe that there's something wrong. Well, now, the recount is just push a button, it prints out the same thing, that's the same totals and you can't go any further to see if the machine was really working

**WP: This is the stuff that Rush holt's bill is aiming to try to deal with?**

RM: Yes. Why do we even have laws on the books in all the states that say that you can have a recount when what they're respectively saying is, sorry you lost, sore loserman, just shut up and go away and don't bother me any more. And that's exactly what's going on.

DD: I agree with Rebecca. I'm sick of hearing this stuff. We're not talking about baseball games here. This is the foundation of democracy. I think a candidate has a duty to his supporters, if he believes there's anything wrong with an election, to go in there and find out if there's anything wrong. And in fact, he or she has a duty to democracy to do that. We all want to believe that election is fair. Unless we go in and audit those things occasionally, we're not going to know that.

BS: I also want to make a comment on the Rush holt bill. I think, the Rush holt bill is the only chance we have for the '04 elections, because these machines are already in widespread use and being purchased. As we know, Maryland just purchased some DRE's and other places from Diebold. Georgia has them, and so these machines are in widespread use already. And they are going to be used in the '04 election and the only hope we have that get something, get these things fixed.

One of the things that worries me about Rush holt's bill is, as of now, I don't know about today but I think probably still today, all of the endorsers are Democrats. One of the pleas I would make to the people who read your article is to really work at making this, to fight it, and keeping this a non-partisan issue. Try to bring more Republicans into the Rush holt bill and whatever they do, don't make this into a partisan issue because if it becomes partisan, that's the kiss of death, in my opinion.

DD: Because the Democrats are already pretty much outnumbered so if it's something with a big D stamped on it, it's going to get killed.

BS: I don't want to put this in a negative way and say, we don't know. We know that there are Republicans who feel this way and so the main thing is that we've got to get them to sign up. That's all. We're not asking anybody to do anything which is un-American. In fact, this is sort of quintessential American. This is what the country's all about. But people need to contact their Congressman and let them know that they need to sign onto this bill. And Senators.

**WP: I'll ask the obvious stupid question. Are you trying to drag the electoral process back two centuries by bringing this stuff up? Because that's the charge that has been made against you.**

DD: No. I just want an electoral system I can trust. And I think everybody else in this country wants it, too. I happen to have the technical background to be quite confident that there's no reason to trust the machines that we're deploying now. So I'm raising the concern. I think there may, in fact, be super-high-tech solutions to this problem in the not too distant future that provide much better election security than we have now. And are significantly less difficult to deal with than maybe some of the solutions we're talking about. So I'm certainly not against technology since I marinate in it to the exclusion of all other activities.

BS: We are also all doing this pro bono, and you can't believe how many hours this stuff takes. We are the ones out there fighting to preserve our democracy. That's what I think we're doing. We are the ones fighting to preserve our democracy.

DD: You know, being an engineer involves making choices about the appropriate use of technology. It is not using the highest tech solution to every problem, whether it's appropriate or not. It's focused on solving the problem by the best means that are available. The best engineers will use the best means that are available even if they don't involve any significant technology at all. I think it's the responsibility of everybody in technology to weigh in with their opinions about the appropriate use of technology and the inappropriate use of technology. And I think it's particularly important for academics and educators to do that. I think part of our job in universities is to try to advise the rest of society, and the policy makers, of what the right things to do are. And to share our expertise and that's really what we're trying to do.

My greatest worry is really an erosion of confidence in the elections. When people can no longer trust the elections I think that that will undermine the legitimacy of everybody in government and I wouldn't like to see that happen.

BS: The confidence is very important. I also fear that if there is the capability of undermining elections sooner or later. Somebody will exploit this technology to steal an election. And to me, our democracy and our right to vote and our right to choose the people who run this country is fundamental and if I feel we've lost that then what makes this country special is gone.

RM: My feeling is that it is a bamboozling of the American public. We're trading away a lot of the checks and balances that we have always had in elections. We're trading this off for high-tech, for faster returns, and it's not true, what we're being told is not the full truth about what is actually going on and I think that we're giving away much more than we're getting. We're giving the opportunity to have an entire election stolen, just because of bad code, not even stolen, just screwed up, fouled up.

DD: We're driving too fast along the side of a mountain road with no guardrail. And maybe you won't go over the side or maybe you will. Do you want to risk it? If you do it long enough you'll eventually go off the mountain.

David L. Dill is a Professor of Computer Science and, by courtesy, Electrical Engineering at Stanford University. He has been on the faculty at Stanford since 1987. He has an S.B. in Electrical Engineering and Computer Science from Massachusetts Institute of Technology (1979), and an M.S and Ph.D. from Carnegie-Mellon University (1982 and 1987). His primary research interests relate to the theory and application of formal verification techniques to system designs, including hardware, protocols, and software. He has also done research in asynchronous circuit verification and synthesis, and in verification methods for hard real-time systems. He was the Chair of the Computer-Aided Verification Conference held at Stanford University in 1994. From July 1995 to September 1996, he was Chief Scientist at 0-In Design Automation. Prof. Dill's Ph.D. thesis, "Trace Theory for Automatic Hierarchical Verification of Speed Independent Circuits" was named as a Distinguished Dissertation by ACM , and published as such by M.I.T. Press in 1988. He was the recipient of an Presidential Young Investigator award from the National Science Foundation in 1988, and a Young Investigator award from the Office of Naval Research in 1991. He has received Best Paper awards at International Conference on Computer Design in 1991 and the Design Automation Conference in 1993 and 1998. He was named a Fellow of the IEEE in 2001 for his contributions to verification of circuits and systems.

Rebecca Mercuri is the founder of Notable Software and Knowledge Concepts. Her management skills have been applied to day-to-day operations as well as product development. As a computer scientist, she has been employed by and consulted for many Fortune 100 firms, including AT&T Bell Labs, Intel, Merck, and RCA. Her specialties are interactive systems (multimedia, digital audio, computer graphics), microprocessor applications (real-time and distributed systems), computer security and forensics. An avid educator, Rebecca has taught in various capacities at colleges and universities in PA, NJ and NY, and she has written and presented training courses for industry and government agencies, including the Federal Aviation Administration, the Philadelphia Stock Exchange, and SRI's Sarnoff Center. She publishes extensively, and is interviewed and quoted frequently by the media (including the Associated Press, National Public Radio, New York Times, Wall Street Journal, U.S. News & World Report, The Economist). Dr. Mercuri holds Ph.D. and M.S.Eng. degrees from the University of Pennsylvania as well as a M.Sci. from Drexel University.

Barbara Simons was President of the Association for Computing Machinery (ACM) from July 1998 until June 2000 and Secretary of the Council of Scientific Society Presidents in 1999. ACM is the oldest and largest educational and technical computer society in the world, with about 75,000 members internationally. In 1993 Simons founded ACM’s US Public Policy Committee (USACM), which she currently co-chairs. She earned her Ph.D. in computer science from U.C. Berkeley in 1981; her dissertation solved a major open problem in scheduling theory. In 1980 she became a Research Staff Member at IBM's San Jose Research Center (now Almaden). In 1992 she joined IBM's Applications Development Technology Institute as a Senior Programmer and subsequently served as Senior Technology Advisor for IBM Global Services. Her main areas of research have been compiler optimization, algorithm analysis and design, and scheduling theory. Her work on clock synchronization won an IBM Research Division Award. She holds several patents and has authored or co-authored a book and numerous technical papers. Recently, Simons has been teaching technology policy at Stanford University. Simons is a Fellow of ACM and the American Association for the Advancement of Science. She received the Alumnus of the Year Award from the Berkeley Computer Science Department, the Norbert Wiener Award from CPSR, the Outstanding Contribution Award from ACM, and the Pioneer Award from EFF. She was selected by c|net as one of its 26 Internet “Visionaries” and by Open Computing as one of the “Top 100 Women in Computing”. Science Magazine featured her in a special edition on women in science. Simons served on the President’s Export Council’s Subcommittee on Encryption and on the Information Technology-Sector of the President's Council on the Year 2000 Conversion. She is on the Board of Directors of the U.C. Berkeley Engineering Fund, Public Knowledge, the Math/Science Network, and the Electronic Privacy Information Center, as well as the Advisory Boards of the Oxford Internet Institute and Zeroknowledge, and the Public Interest Registry’s .ORG Advisory Council. She has testified before both the U.S. and the California legislatures and at government sponsored hearings. She was runner-up in the first election for the North America seat on the ICANN Board. Simons was a member of the National Workshop on Internet Voting that was convened at the request of President Clinton and produced a report on Internet Voting in 2001. She also participated on the Security Peer Review Group for the Department of Defense’s Secure Electronic Registration and Voting (SERVE) Project.

Further data on this issue can be found here:
http://www.verifiedvoting.org
http://www.verifiedvoting.org/fair_elections.asp
http://www.notablesoftware.com/evote.html
http://www.blackboxvoting.com/

---

*William Rivers Pitt is the Managing Editor of truthout.org. He is a New York Times and international best-selling author of three books - "War On Iraq," available from Context Books, "The Greatest Sedition is Silence," available from Pluto Press, and "Our Flag, Too: The Paradox of Patriotism," available in August from Context Books.*

-------

**Jump to TO Features for Monday 20 October 2003**

Today's TO Features ▼