Chapter 9
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

9
Noun *and* Verb

So, what or who is rob-georgia?

When you interview voting system officials, you spend twice as much time following up on their dodgy answers as you do asking the questions in the first place. Flip back to page 165, Chapter 8 and take a look at Joe Richardson, who I believe you might also find in *Webster's Dictionary* defining the word "stone-wall." Compare him with Rob's straight-talking interview.

Meet Rob Behler:

Harris: "What was your position with Diebold in Georgia?"

Rob: "I was a server technician and then Product Deployment Manager for the Georgia project."

Harris: "What was the FTP site for?"

Rob: "One of problems we had was an issue with the GEMS database. They had to do an update to it, so they just post the update to the web site."

Harris: "What was rob-georgia?"

Rob: "I believe what that file was for, I did a — well, there were a ton of holes with the programs on those machines. When they all came into the warehouse, I did a quality check, this was something I did on a Saturday. I found that 25 percent of the machines on the floor would fail KSU testing —"

Harris: "What is KSU testing?"

Rob: "Kennesaw State University. We knew basically what they would be testing and the trick was to make sure the machines would pass the testing. So I went and checked a pallet and found it was bad. And I checked another, and another, and I knew we had a problem...

"I'd come in on a Saturday, I had two of my sons with me, and I thought I'm going to just look. And it was bad.

"Then first thing Monday morning I raised the question, I said, 'Hey guys, we've got a problem — there's 20-25% of the machines that are palletized that are failing..."

How quirky. How did this batch differ from what was certified by the ITA labs, and signed off on by Diebold quality control? Was this just a fluke, or a breakdown in the whole certification and testing system?

Harris: "What kind of problems were you seeing?"

Rob: "...One of the things we had wrong was the date wasn't sticking in the Windows CE. The real time clock would go to check the time on the motherboard, and it would have an invalid year in it, like 1974 or something...

"They had to do an update in [Windows] CE to fix all those dates. So the way we did that in the warehouse was, they would post whatever the update was on the FTP site. James [Rellinger] would go get the file and put it on the [memory] cards. Because you load everything through the PCMCIA cards. You boot it up using the card and it loads the new software...

"I went over to Dekalb [County]. We updated 1,800 machines in basically a day and a half. I still remember ol' Rusty, down at the warehouse, we ended up touching every single machine off the pallet, booting 'em up, update it, we had a couple hundred machines done when in comes a new update over the phone.

Harris: "You mean you used a modem or they called you on the phone?"

Rob: "No. A phone call. They'd say 'Oh no no, the way we had you do, that's not going to work, here's another thing to do. Okay, we just did a few hundred machines, now we gotta do it this way..."

Rob and I discussed how patches were downloaded. For some reason, the techs were told to use their own laptops to download files from the Diebold FTP Web site.

According to Rob, he was instructed by Diebold not to discuss anything with Georgia's voting machine examiner (Dr. Brit Williams) or other state officials. This was awkward, because Dr. Williams was working alongside Rob at times, and when Dr. Williams asked questions, Rob made the mistake of answering. This infuriated Diebold managers. We'll get to the shouting and lying in a minute; but for now, back to downloading those program modifications:

Rob: "They used my laptop. It was not secure, either. They just used the laptop to repro the cards. Diebold never gave us anything with a PCMCIA slot, then they'd tell us, 'Go download this,' so we'd have to get out our own laptop to do it."

Harris: "Who instructed you about the FTP site? Was it a Diebold employee?"

Rob: "It was Diebold."

Harris: "Was it the people in Ohio or the people in Texas?"

Rob: "The people in McKinney [Texas]."

Harris: "Who were some of the Diebold people? Do you remember any names?"

Rob: "Ian. I remember one of the guys, Ian, I can't remember his last name. One of the main guys we dealt with was a guy named Ian. He was actually involved in the design of the motherboard. He was very much involved in trying to figure out how to fix the problems. So they sent us upgrades, but then after we did it KSU still failed a ton of machines."

(Ian Piper was a stockholder in the company acquired by Diebold, Global Election Systems. The staff directory lists him as Manufacturing Manager, Research & Development division for Diebold Election Systems.)

Harris: "As I understand it, they send the system to Wyle labs for certification, and also to Ciber to test the software. But from what

you are describing, I can't understand how the machines got through what they are telling us is 'rigorous testing.'"

Rob: "From what I understand they ended up figuring out that the cards that we were loading that fix that Diebold provided for us, well they were never tested, they just said 'Oh here's the problem, go ahead and fix it.'

Harris: "So what is your opinion about the certification testing?"

Rob: "No, it's not just that. NOBODY even tested it! When I found that out — I mean you can't not test a fix — I worked for a billing company, and if I'd put a fix on that wasn't tested I'd have gotten *fired*! You have to make sure whatever fix you did didn't break something else. But they didn't even *test* the fixes before they told us to install them.

But Dr. Brit Williams told us this is not possible. "After state certification any change to either the Microsoft operating system or the Diebold election system voids the state certification," Williams assures us. "The revised system then must then go back through the entire ITA Qualification and State Certification."[1] And remember, before being shipped to Georgia, these machines go through testing. Rigorous testing.

Rob: "Look, we're doing this and 50-60 percent of the machines are still freezing up! Turn it on, get one result. Turn it off and next time you turn it on you get a different result. Six times, you'd get six different results."

Harris: "Can you give me an example of different results?"

Rob: "Meaning the machine does something wrong different each time you boot it up. One time and it would freeze on you, next time it would load the GEMS program but have a completely different type of error, like there'd be a gray box sitting in the middle of it, or you couldn't use a field."

Harris: "Was this all due to the clock?"

Rob: "I don't know for sure. They [the machines] were not originally doing it. Then they fixed the real time clock, and it was supposed to make it work normal. It fixed the clock problem — the clock problem had caused it to come up and not show the battery at

> one point...I mean, *you don't have the machine plugged in*, you boot it up, and it starts, and says it 'has no battery.' That's like saying, 'this morning I got out of bed and I stood up and I had no brain.'"

A memo from Talbot Iredale dated July 2, 2002 confirms the clock problem. "The new WinCE 3.00 release is now on the FTP site," it says. The memo directs the user to get a file called WCE300-020702.zip, and says that the purpose of installing this modification is to "Fix problem with getting and setting persistent Real Time Clock values," among other things. Iredale instructs the user to "Copy both the fboot.nb0 and the nk.bin files to a PCMCIA card and insert it into the bottom slot and then power the unit on," adding that this process will modify both the bootloader and the WinCE image.

"WinCE image" is a term is used to describe the specialized Windows operating system developed by Diebold for use with its touch screen system. It refers to an operating system, not a picture or an "image" in the traditional sense.

Not only was this modification to Diebold's customized version of Windows CE not certified, but Iredale indicates at one point that he wants to avoid letting Wyle (the certifier for the touch screen firmware) look at Diebold's special Windows source code *at all*. In a memo dated April 15, 2002, Talbot writes: "We do not want to get Wyle reviewing and certifying the operating systems. Therefore can we keep to a minimum the references to the WnCE 3.0 operating system."

Whatever was on the special Windows system cooked up by Iredale and others at Diebold, it didn't seem to work very well:

Rob: "And then when we loaded the software to fix that, the machines were still acting *ridiculous*!

"I was saying, 'This is not good! We need some people that know what this stuff is supposed to do, from McKinney, NOW! These machines, nobody knows what they're doing but Diebold, you need some people to fix them that know what's going on! They finally brought in guys, they ended up bringing in about 4 people...

You'd think that with such troubles, someone might follow standard company procedure and write up a "bug report."

"All bugs ever reported have bug numbers," wrote Ken Clark in a memo dated Jan. 10, 2003, pointing out that the whole collection can be found in "Bugzilla." So I went looking for Bugzilla reports from Georgia. My goodness. They weren't there!

Bugzilla report numbers 1150–2150 correspond with June–Oct. 2002, but although hundreds of these bug numbers are mentioned in memos and release notes, I only found 75 Bugzilla reports for this time period, and none from Georgia. Strange. I was looking forward to reading the explanations about how computers can get up in the morning and announce that they have no brain. Aha! Here's a memo about missing Bugzilla files: It's dated 8 Jul 2002, from principal engineer Ken Clark:

S*ubject*: **bugzilla down, we are working on it.** "We suffered a rather catastrophic failure of the Bugzilla database," he writes. He warns that recovery of the bugzilla reports "will be ugly" and adds that "there will be a large number of missing bugs."

In a follow up note on July 16, Clark says "Some bugs were irrecoverably lost and they will have to be re-found and re-submitted, but overall the loss was relatively minor."

To understand the significance of these two e-mails, you must realize that among programmers, system backups are a religion. People are fired for not performing a daily backup. Some programming shops back up every shift! Because backups are critically important, expensive *automated* tape systems are employed to minimize any data loss. By our estimation, almost a thousand bug reports are missing, including all the Georgia bugs.

Rob: "When the machines came in, they came to us first. They were in the warehouse. We assembled them. They'd come in a box with a touchscreen, and another box with the booth. We assembled the machine and we ran it though series of tests. We'd check the power cord, boot up the machine, check the printer, bar code it, update Windows CE, then send it on to Brit. He did the KSU testing the L&A [Logic & Accuracy] was done at the county level, right before the election."

Harris: "So…the L&A was not done at acceptance testing?"

Rob: "It got so there wasn't time. They did it before the election."

Now, supposedly, this L&A testing procedure is kind of a "mock election" which you do by entering practice votes. I pictured people pushing the touch screen, and wondered how many test votes you push before your finger gets really tired. Not that many, apparently:

Rob: "The L&A testing — You would just enter, like, one vote and — you just choose one — you don't need to be specific on which one.

I see. One vote. But then I found out that some of their L&A test involves no touching at all:

6.1. Test Count

- performing a manual Logic and Accuracy Test
- performing an automated Logic and Accuracy Test

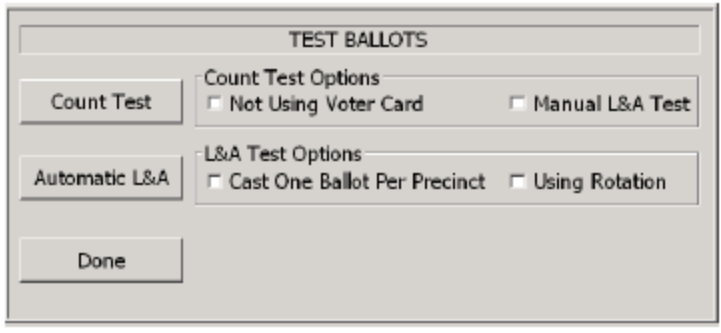


Figure 6-2: Test Ballots Screen

Ballot Station Users Guide: *"The automatic L&A test, on the other hand, allows a pre-determined combination of ballots to be automatically selected and marked, according to the voting options selected."*

Rob: "I worked there from mid-June to mid-July. The whole time they were upgrading the software and doing some sort of fix to it..."

"You've gotta go take care of this JS [junk shit] equipment, I told them. Finally, I raised it as high as you go, I raised it to Bob Urosevich, he's the head of it. [Urosevich is President of Diebold Election Systems] I told him personally, 'This is bad, I don't see us putting an election on with these machines!'

"That's where they finally assembled the teams. They got some big ol' vans, we loaded up as many people as could fit in.

Question: Who paid for the vans? Diebold?

Who paid for the people piling into the vans?

Because now I'm having a hard time understanding why Diebold says it "had no indication" that these patches were done at all. Perhaps Diebold spokesmen can check with their own accounts payable department and then provide us with thorough, honest, and forthright answers about the Georgia program modifications.

If a private company, like Diebold, asserts its right to secret control of the public voting process, is it too much to ask for such a company to answer questions? I'm sure I am not the only one who finds this behavior intolerable.

Rob: ..."And then you know, ironically, later on right before I exited, they were scrambling for a date, they were trying to get us, the teams, into Fulton County to do Fulton County's 1,900 machines.

"They were in the most horrific spot. The place they warehoused them was like 1900 machines in a little office space, there was no way we could get at them. The machines are like 58 pounds, and they had to bring them in unstack them off the pallet, restack on the pallet, talk about labor, talk about wasted money! It's like a warehouse and offices off 75, in Atlanta, I'm talking to this guy he's a great guy, he's from Fulton County. Him and I were scheduling this, figuring it out how to get to these machines and

> do the update before KSU has to test them. We cannot be doing this at same time as KSU ...
>
> I go back to the office. Brit [Dr. Britain Williams] was there, and he says 'What's it look like for Fulton?'
>
> I said 'There's no way were going to able to get to Fulton County by Thursday.' I said we could probably be out there by Friday or Saturday. He said 'There's no way we can do it at the same time, you know that....'"

But Dr. Brit Williams, when interviewed by Kim Zetter of *WiredNews,* "denied that Rob ever mentioned patches to him and said, to his knowledge, no uncertified patches were applied to the machines. He said he would be very concerned if this happened."[2]

He should be concerned, because if Rob's story is correct, Diebold may have violated federal regulations. Patching systems after they've been certified opens the possibility for malicious code to be installed into the voting system, altering the results — which is precisely why it is against the law. The results of any election that used patched Diebold systems might be called into question.

The scenario that Dr. Williams has been reporting to state officials just does not correspond with what we are learning from Rob. Williams writes:

> "Overall security of any computer-based system is obtained by a combination of three factors working in concert with each other:
>
> "First, the computer system must provide **audit data** that is sufficient to track the sequence of events that occur on the system and,to the extent possible, identify the person(s) that initiated the events."

But in the next chapter we will blow up the audit procedure.

> "Next, there must be in place well defined and strictly enforced policies and procedures that **control who has access to the system**, the circumstances under which they can access the system, and the functions that they are allowed to perform on the system."

I must have missed the section of the operating manual that describes people piling into vans and driving around updating voting programs with uncertified patches, using cards they made on their own laptops.

"Finally, there must be in place **physical security**; fences, doors, locks, etc.; that control and limit access to the system."[#]

Well at least they have our voting machines under lock and key.

Back to the interview:

Rob: "They were actually swapping parts out of these machines that were on site. They'd cannibalize a machine with a bad printer or whatever, they'd grab the screen off of that to put on another machine with a failing screen, they'd retest it. They were not just breaking them down, they were taking pieces off and putting it back together.

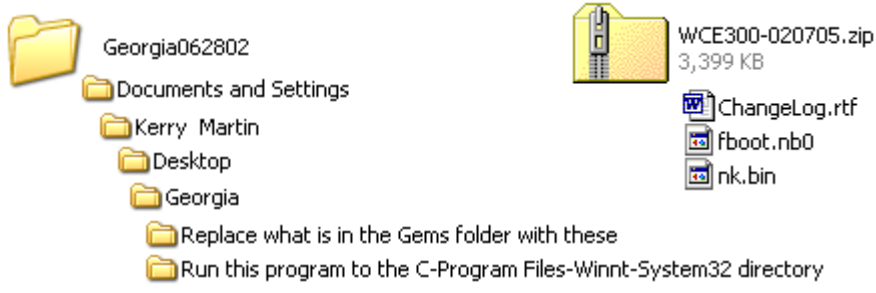
"Even the machines that are updated, that had the right release of the software, exactly like the company wanted it, you'd boot it up and all kinds of crazy things would happen. That led to my belief that when voting took place, there would be problems."

Harris: "Do you remember what release number it was?

Rob: "Release — I don't remember the number because what they did was it was always the date...

"The date was...let me see...**June 28**. No, the last one, the date that was supposed to be on there was **July 5**.

Rob: "There was about three updates, the CE software, the date that would come up would be the last. After that they came up with another fix, that's the August one at that point.



These files were found on the Diebold FTP web site in January, 2003.

The more you examine this "electronic patch" thing, the more out of control it looks. From the memos, it appears there were so many patches that the garment might have changed color altogether:

Date: Thu, **13 Jun 2002**
Subject: WinCE 3.00 June 7th Release
From: "Talbot Iredale"
"The new WinCE 3.00 and bootloader are on the ftp site. The file is WCE300-020607.zip...

Date: Tue, **2 Jul 2002**
Subject**:** WinCE 3.00 July 2, 2002 Release
From: "Talbot Iredale"
"The new WinCE 3.00 release is now on the ftp site. The file is WCE300-020702.zip..."

Date: Thu, **4 Jul 2002**
Subject**:** WinCE 3.00 July 04, 2002 Release
From: "Talbot Iredale"
The new WinCE 3.00 release is now on the ftp site. The file is WCE300-020704.zip

Date: Fri, **5 Jul 2002**
Subject**:** WCE 300 - July 05, 2002 Release
From: "Talbot Iredale"
"...This is fixed in the July 05, 2000 release which is now on the ftp site."

Date: Thu, **8 Aug 2002**
Subject**:** WCE 300 - Aug 08, 2002 Release
From: "Talbot Iredale"
"The WCE300-020802 release is on the ftp site."

Date: Wed, **9 Oct 2002**
Subject**:** AV-TS R6 Bootloader and WinCE version numbers
From: "Ian S. Piper"
"...another method for determining the version number of the install files, prior to installation, is to view the creation date of the file on the flash memory card and compare it to the list below. (Unless you trust that someone has labeled the flash card correctly.) ...I've created a list of the file creation dates, and their versions...

Bootloader (filename "fboot.nb0")
Mar. 14th, 2001 Rev 1.00
Jan. 28th, 2002 Rev 1.01
Jun. 7th, 2002 Rev 1.02

Windows CE Image (filename "nk.bin")
May 25th, 2001 WinCE 2.12
Jan. 28th, 2002 WinCE 3.0
Jun 7th, 2002 WinCE 3.0
Jul. 2nd, 2002 WinCE 3.0
Jul. 5th, 2002 WinCE 3.0
Aug. 8th, 2002 WinCE 3.0

He adds, "Someone with the BallotStation install file archives can create a list of BS [Ballot Station software] versions if they want to bother."

There were more patches — the "clockfix.zip" patch is a little addition dated July 7, 2002. According a memo dated Aug. 6, 2002, Kansas may have caught a few bugs from Georgia:

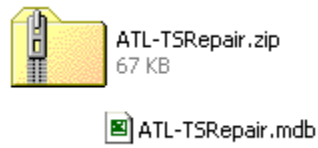
Tuesday, August 06, 2002
Steve,

"It was believed that only units built for Georgia would be affected. However, Lesley had 38 units shipped to Johnson County around the same time, so she was affected as well. There should be no others (famous last words)..."

The techs were stitching new updates into the voting machines right up to Nov. 5, 2002 — Election Day, and apparently, even after the election:

The date on this file is Nov 11, 2002 — just six days after the general election. The file it appears to be "repairing" corresponds with the database used to count the touch screen (TS) votes in GEMS.

It is passworded and I have not opened it, and therefore don't know what kind of repair it is making.



Certification Requirements Summary

Governing Entity	Certification Required	Need NASED #	Need Wyle Cert	Need CIBER Cert	Modification Requires Recertification	Submission Form Required	Technology Escrow Required
Alabama	☑	☑	☐	☐	☑	☐	☐
Alaska	☐	☐	☐	☐	☐	☐	☐
Arizona	☑	☐	☐	☐	☐	☐	☐
Arkansas	☑	☐	☐	☐	☐	☐	☐
California	☑	☑	☑	☑	☑	☑	☑
Colorado	☑	☐	☐	☐	☑	☐	☐
Connecticut	☑	☑	☐	☐	☐	☐	☑
District of Columbia	☑	☐	☐	☐	☐	☐	☐
Florida	☑	☑	☐	☐	☑	☐	☐
Georgia	☑	☑	☐	☐	☑	☐	☐

This document was found in a file from the Diebold FTP site

...Rob: "...This is an example we did: We would plug it in, boot it 3 times, unplug it, boot it three more times. I wrote a sheet on this.

"This guy came in from McKinney, he was about the second in command. He's a good friend of Bob Urosevich. About second to Bob, at least now, he got a promotion. Greg? Something like that. He flew in and I went to Dekalb and I tested and together we went through, and we wrote down every single error, and he booted them himself, and was looking at the results and seeing how sporadic they were. and we found out of the machines we tested, about 75% of the machines had different sporadic things. He was working with me and we were writing them down, we literally wrote everything down."

" — Greg Loe is his name. [Greg Loe, Contoller] I drove him out there. Brit [Dr. Britain Williams] was there, KSU was doing their testing. **They were bombing these machines out left and right.**"

"I'm telling him, 'They're all like this.' At this time I was working 150 hours in 2 weeks I was there all the time with these machines, that's the reality of it. The techs were working overtime trying to fix them. We couldn't get enough from the factory because so many were bad. You'd get a shipment of 300, but 75 were bad, they couldn't put them out fast enough to replace all the defects...

..."Harris: "I understand they did a big demonstration during the summer, with the machines."

Rob: "I was there when they told me I needed 1100 machines for a demo. I thought, 'The trick is coming up with 1100 machines that actually work.."

Harris: "Do you know who was writing the fixes?"

Rob: "He had a weird name. He came out of Canada...— That's it! Talbot Iredale, [he] would actually fix it and say, 'Oh, here's the problem,' and stick it on the FTP site we'd grab it stick it on the card and make a bunch of copies and use it."

"...They produced it and got it to us in 24-48 hours. If I'd known they hadn't tested it I simply wouldn't have installed it! My background tells me that's a no-no...

Let's revisit the concept of locks, keys, fences and warehouse security

...Harris: "How secure were the machines, from what you saw?"

Rob: "I'll tell you something else — we didn't have badges — people could just walk right in and get to the machines."

... **Harris:** "Do you think anybody could have tampered with a machine, if they wanted to?"

Rob: "Well, when we did the quality control check we'd open it up, they have a little box for the printer. We would find the key still in the printer. Someone could literally take that. We found cards left in the machine. [Voter cards activate the vote; memory cards store the votes.] I wondered what would happen if the wrong person got it..."

Harris: "Were there any protections to keep you from duplicating memory cards, or to have them serial numbered or whatever?"

Rob: "The memory cards, you can just duplicate them. You have to have the proper info on the card, for the machine to boot up, but you can just make copies of the cards."

If what Rob is describing sounds pretty slipshod to you, you're not alone. In a September 2003 letter by a member of the Georgia Elections Board to Cathy Cox (Secretary of State), we learn that voting machine security is rather lacking.

"A missing DRE (*touch-screen voting machine*) for the State Board of Elections is tantamount to a missing ATM for a bank," J. Randolph Evans states in his letter. He then goes on to report that voting machines have been found in hallways, stairwells, and trunks of cars.[3]

* * * * *

Now every good fiasco has a little shoutin' and lyin' — and this one has it all — office politics, regular politics, and people scrambling to protect the company checkbook.

Harris: "When I asked Diebold if there was anyone named Rob in Georgia, they said no. Did they know about you?"

Rob: "They knew me and they knew me well. I met Bob Urosevich [President of Diebold Election Systems] a couple different times, and Ian, and then Greg Loe, he got promoted, he was basically Bob's right hand man..."

"You know one of the main things that really just made me so upset, they were just like, 'This Brit guy, don't even speak to him, it's a political game, you've gotta play the politics.' Well, he walks in and says 'What are you guys doing?'

"I said, 'We're putting in an update.' He said, 'Will it change what it does?' We said, 'Just do your normal test, we're supposed to get the machines ready for you.'

"He tells someone at the office and they freaked out. They were like, 'What the heck are you doing???'

"I wasn't supposed to talk to him at all, I guess. The guy had a flannel shirt on, he was kicking it and he was very genuine and open and there we are in the same room together, but because I actually spoke to him I got reprimanded. They said, 'If they ask you any question, you gotta say 'Talk to Norma, to one of us...''

Harris: "What did you say to him, anyway?"

Rob: "He [Williams] said he wanted to talk to me, so I met him in this little side office and asked me what was going on. I basically said I was updating the machines, doing a quality check making sure the machines are the same, making sure they had the the right release of windows.

"Essentially, when I got back there was a meeting called. Urosevich was in it with a conference call. I went in, la-dee-dah, thinking I'd been doing a great job and it caught me by surprise. It just totally blew me away that they would be so incensed, and just absolutely angry about something so frivolous as the basic information I gave Dr. Williams. I've never been told to shut up so many times by so many people."

Harris: "You mean, 'shut up in this meeting,' or 'shut up' by not talking to other people?"

Rob: "I'll tell you exactly, I'll give you a quote — this came from Urosevich: He said 'We don't need *you* airing our dirty laundry!'"

"It was during that meeting the details came to light for me about patches and certifying them. I wasn't aware of that before. There was this big discussion about what needed to be certified. In the course of trying to determine whether they needed to be certified, they were saying 'What do we tell Kennesaw State?' Everybody went around and gave opinions except for James Rellinger, who didn't know. Wes [Krivanek], Norma [Lyons], Darrell [Graves], Bob [Urosevich] on the phone, each gave opinions on how it should be spun as to what we were trying to do. During the course of the conversation I said, 'Can't we just tell them? What's wrong with that?'"

"[they said] 'No no you can't do that, it may be a certification issue!' We were sitting around tables with Urosevich on speaker phone, trying to decide whether to tell the truth, half the truth, or a complete lie."

Georgia had just ordered up $53.9 million in voting machines, and the ink on the check wasn't quite dry.

"If they started erring in mass quantities, Kennesaw State's going to raise a red flag, the secretary of state's going to raise a red flag and Diebold wouldn't get paid," Behler told Kim Zetter, of *WiredNews*. "'I understand if a company has information they need to keep under tight lip. But when you sit around discussing lying to a client in order to make sure you're getting paid . . . it's an ethics issue."

> **Rob**: "The rumor around the office was that Diebold lost maybe $10 million on the Georgia thing. I mean, they only sold the machines for what, $2,000, or $2,500, and then you have to build them and then you're paying people $30 an hour and you are out touching 22,000 machines *four times* — there's no way they didn't lose money on this deal...
>
> "The jist of the conversation was, you screw around with this and they might decide not to pay us."

How credible is Rob Behler?

Dr. Brit Williams told *WiredNews* that Rob was a disgruntled employee who was fired from the project by Diebold and Automated Business Systems and Services.

Rob's personnel records discredit this assertion.

"'He was released because his part of the project was completed,'[ABSS vice president for the southwest region Terrence] Thomas told *WiredNews*, explaining that it was not a performance issue.

James Rellinger, a Diebold contractor who worked with Rob, also rejects Williams' interpretation of events. Rellinger told *WiredNews* that that both Diebold and ABSS seemed happy with Rob's work.

But there are additional reasons to believe Rob:

• I spoke with Rob in March 2003. He had no way of knowing which files were sitting on the Diebold FTP site in January 2003 — yet in his interview, he mentions specific electronic patch files, and I was able to find the files he mentioned among those on the Diebold web site. The file dates matched exactly, and the information in the accompanying release notes support Rob's story.

• Rob could not know that internal memos from Diebold would surface. He recalled that people with the names "Talbot Iredale" and "Ian" were involved with the fixes. Now we know that memos authored by Talbot Iredale and Ian Piper reveal patches just like those reported by Rob. These 2002 memos, which were revealed in Aug. 2003, contain 13-character passwords for the matching files on the Diebold FTP Web site — files which had never been opened because they were locked with complex passwords. The passwords in the memos open the patch files found on the FTP site in Jan. 2003.

• I interviewed Rob in March 2003; Kim Zetter from *WiredNews* interviewed him in September 2003; I interviewed him again in October. He never evaded questions and his answers stayed consistent over this six month period.

• Rob was told to download information to his laptop. He has saved several files. He has the notes taken while demonstrating problems to Greg Loe, and has provided a copy of his notes (and a videotaped deposition) to a lawyer who is working on a case with Georgia activists.

Rob: "...I went into this Diebold thing with no real knowledge of the voting industry. When I left, I not only had a complete grasp, but I had a complete disrespect for these machines.

"And with the folks in the office who were so — you know, 'I'm the political person, you have to know how the system works' — they were so much more concerned about their own self importance, they were losing track of *do the machines count the vote properly*!

"Because that's what the people in Georgia need.

"And I'm one of them."

Rob jeopardized his employment future by stepping forward to tell us what really happened in Georgia. He has never asked for anything. This is especially impressive when you learn about a method that citizens like Rob can use to enrich themselves (albeit, at the expense of the public interest).

In cases where a government agency has spent taxpayer money based on fraudulent claims, the first citizens to file a "Qui Tam" lawsuit collect as much as 30% of the money mispent by the agency in question — in this case, for Georgia, nearly $54 million. The catch? The case must be filed under seal. No congressional investigation, no public disclosure, just a secret filing that may or may not get unsealed.

But citizens need to know the details about these voting machines. There are bills pending in congress and states considering purchase as of this writing. Secreting the evidence away, so that a few citizens can line their pockets with millions (and sidestep liability, in the process, while leaving honest citizens, like Rob, hanging out the window), just seems wrong.

I told Rob about Qui Tam, and suggested that he consult someone for guidance to decide whether to pursue this path. He did. He consulted the Bible. He looked up what the Proverbs have to say, and shared their wisdom with me.

"I'm not interested in it," he decided. Now, Rob Behler is a man who is raising seven children, with little material wealth. He could probably use 30 percent of $54 million. Instead, he has chosen to protect the security of your vote by telling the truth, publicly. In Rob, from Georgia, we meet the kind of quiet, patriotic citizen that makes us proud to be Americans.

Rob-Georgia: Epilogue

Harris: Do you remember the date when you got this job back in June?

Rob: Yes. June 24.

Hmmm.

Harris: Are you sure it was June 24?

Rob: Yes. June 24 to July 29.

Date on the rob-georgia files: June 4.

Twenty days *before* Rob was hired.

Back to square one. Who or what is "rob-georgia?"

Chapter 9 footnotes

1 – "Security in the Georgia Voting System," April 23, 2003, by Britain J. Williams, Ph. D.

2 – *WiredNews.com*, 13 Oct. 2003; "Did E-Vote Firm Patch Election?"

3 – *Georgia Vine* Vol. III, Issue 18, 25 Sept. 2003.

Aug 18, 2003:
2004 Presidential election was offered for sale on E-Bay.
Asking bid: $99,999,999.99