Chapter 3
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with
David Allen

Edited by
Lex Alexander

Cover Art by
Brad Guigar

3
How Do You Verify Voting Machine Accuracy?

If we solve this problem, the rest of this book is moot. However, before we get to solutions, two things:

1) I keep saying we can't verify the accuracy of these things. What do the voting machine companies have to say about this? How do our politicians explain it? We should at least listen to the company line, so the first part of this chapter will discuss the official explanations.

2) If you are in the high-tech community, you may be just dying to suggest technological solutions. Before you start explaining that cryptography, redundant systems, or a secret pin number are the answer, let me explain: Cryptography doesn't solve the problems either nor does redundancy or a receipt with a pin number.

But don't just take my word for it — We have included a discussion of open source and other technological solutions later in this book.

We put this chapter here, because after reading the little shop of horrors in the previous chapter, you might want to hear some good news. And to cut to the chase: We favor a hybrid system — touch screen machines with a voter-verified paper ballot, with an audit that compares the two against each other.

The official line on voting machine verification:

Indeed, they can't be properly audited, but what you'll hear from the manufacturers is this: "Each machine creates an internal facsimile of each vote, and if there is any question, we can simply print out each vote for a hand recount."

And what about the voter being able to see that his vote was recorded the way he cast it? Well, absolutely, the voter verifies his vote, they tell us. After making his selection for each ballot question, the votes appear on the screen and the voter confirms his choices.

Saying the machine creates an internal facsimile of each vote is just a fancy way of saying that the data in the machine can be printed out one vote at a time. Think of it this way: Suppose you have an address book on your computer, and it lets you print a full page with a single record, or a list of all the records. Now, suppose you have an error in your computer records, and instead of "John Doe," you typed "Joxn Doe." Whether you print his record as a single page, or you print out a list, he will appear both places as the erroneous "Joxn Doe."

If incorrect programming caused the machine to record your vote for Truman as a vote for Dewey, it's not going to help to have the machine print a copy of its own incorrectly recorded vote.

Now let's look at the "voter verified" issue. It's nice that you can review your choices and confirm them. However, what you are looking at is just a screen display. The screen says "Voted for Truman, correct?" — you press "Confirm" — but that does nothing to prove that the software inside the black box instructed the memory card to record your vote correctly.

The solution is simple: All major voting machine manufacturers say they have machines capable of printing ballots. From the beginning, Avante and AccuPoll have provided touch screen machines that print a paper ballot. If the machine prints a ballot that shows your vote: "Truman" but inside the machine, the software interprets your vote as "Dewey," all we have to do is devise a way to compare the paper ballots, which you have independently verified, to the machine counts, and the machine miscount will show up.

Optical scan machines have ballots, but if we don't look at them, we can't say we verified the machine count. Running the ballots through the machine again won't prove anything — if the software is programmed incorrectly, the same error will probably appear when you run it through a second time. Running it through a different machine may not help, either — if both machines use the same software, they might both give you the same error.

Another answer you'll hear is that we don't need to compare the paper ballot, which you have verified, with the machine tally, because the voting system has been so carefully tested. That claim is debunked in the Chapter 5.

Why is comparing the paper trail to the machine count so important?

When you verify the accuracy of a count — points in a beauty pageant, dollars in your bank account, or votes cast in an election, it is called doing an *audit*. So

what, exactly, is an audit? Can we just make up our own rules as we go along? Who has expertise in proper auditing procedures?

Auditing is an accounting function. Proper auditing include the following:

• Independent data sources

• Transparency (meaning the accounting process is transparent to everyone)

• For systems that are part of the public commons, like voting, scrutiny by "many eyes"

Computerized vote-counting systems fail on all of these criteria, but this is easily correctable, if we take appropriate actions.

Comparing two <u>independent</u> data sources

In auditing, you prove one set of data is correct by verifying it against a matching set of data that comes from a different source.

Example - Paying taxes:

Tax authorities require you to keep independent verification.

1) You fill out a report when you file your taxes ("Source 1"). You may keep a computerized record of your deductible expenses and your expenditures, using a program like *Microsoft Money*. ("Source 1a"). Why are these two sources not independent? Because only one person (you) has verified them.

2) You also have independent records, like bank statements (verified by your bank) and receipts (verified by the vendor) ("Source 2").

To do a proper audit, the IRS uses your tally, but backs it up with a document trail that is verified independently, by banks and vendors.

Independent Auditability in Voting:

Punch card and optical scan systems

1) You enter your vote on a punch card or optical scan ballot. This is "source 1"

2) The actual record containing your intent is counted by a software program on a computer. This is "source 2."

3) No one, however, is allowed to look at source 1. We can only look at source 2, the computer tally.

As described above, the vote count is never verified at all. Although we have two independent sources, we refuse to allow anyone to look at a more important source, the voter-verified ballot. Using this system, we cannot know whether the machine is correctly recording our votes.

However, we can easily correct this problem by regularly, thoroughly comparing the computer count with a hand-count of the ballots.

Touch screen, DRE, Internet and vote-by-phone systems

1) You enter your vote into a computer, using a touch screen, keyboard buttons or a wheel. The screen, or the phone system, provides a digital representation of your vote and asks you to confirm it. However, you cannot see your vote actually being recorded. (Source 1)

2) The computer transmits your vote to a second system, creating a redundant record in case the power goes out, or so that people can look at another version of the vote repository. (Source 1a)

3) The computer tallies up the votes that it recorded. (Source 1b)

4) The computer prints a summary of the votes, and the election official uses this summary to represent the physical record of the vote (Source 1c)

5) The computer also can create a facsimile of each vote it has recorded, an individual "ballot" for each vote cast. (Source 1d)

Note that the system just described is not auditable, because it does not keep any record verified by any party independent of the computer.

Asking you to "verify" your vote by saying yes to a computer screen is exactly the same, in terms of data integrity, as asking you to tell an election official your vote, which she then asks you to repeat while never letting you see what she wrote down. That procedure is absurd and would be trusted by no one, yet it is exactly equivalent to the touch screen system.

If the touch screen prints a ballot that you verify, which is saved in a secure ballot box, a proper audit can be done by comparing the machine count (source 1) to the voter-verified ballots (source 2).

Transparency

Proper auditing requires transparency. Just ask an IRS auditor whether you can get by with handing him a shoebox full of indecipherable receipts with no explanation. Not likely. You either have to organize it and explain it clearly, or it gets thrown out.

Transparency somehow evaporated when we privatized our vote-counting system.

Discrepancies they cite are explained away by technicians who are not sworn election officials citing "glitches" in the programming that we cannot see. Sometimes technicians fly in to "replace a chip" (yet we have no idea what's on the chip). In one news account, in which logs showed 48,000 votes cast, but only 36,000 recorded, a technician *e-mailed* the "correct" results for the missing votes, claiming it did not change the outcome, though no one would ever know, because an audit trail didn't exist.

Trust is critical, so transparency is especially important. The Declaration of Independence does not say "Governments are instituted among men, deriving their just powers from the consent of the computer programmers."

No matter how clever the cryptography, no matter how great the open source program is, unless ordinary citizens with no computer expertise can see with their own eyes that votes are being counted accurately, the audit system fails the transparency test.

In a democracy like ours, you don't need to be a lawyer to sit on a jury. You shouldn't need to be a computer programmer to count a vote.

scottxyz
DemocraticUnderground.com

"Many eyes"

The "many eyes" method is a great way to eliminate conspiracy and prove that a system is trustworthy.

Elections are simply no good unless we believe they are accurate. The Soviet Union held elections while under communism, but no one believed they were valid. According the *London Guardian*, Saddam Hussein held elections, too and reported that he had garnered 100 percent of the votes. I assume that no one wants elections like these.

"Many eyes" simply means that we let as many independent parties as possible view the vote-counting. The more eyes on the count, the less room for shenanigans. We do not want a system that only a few software engineers can verify. We require something that you, I, the mailman and our kindly senior citizen volunteers can attest to. "Of the people" does not also say, "as long as they are computer programmers."

I spoke with Christopher Bollyn, a reporter who has written several articles about the erosion in integrity of our voting system as it migrated to computerized counting. He described an election he witnessed in France which illustrates "many eyes" perfectly:

- Voters cast ballots on paper, and when it comes time to count, the room becomes crowded with citizens.
- As many citizens as can fit in the room are allowed to watch the counting. Sworn election officials, some from each party in the election, in front of all the observers, count the ballots into piles of 100.
- Each set of ballots is placed in a bag.
- Then, one bag at a time, the election officials count the ballots, announcing each one.
- They tally up one bag and move to the next, until all are done.
- It takes a relatively short time to count 1,000 votes, and by having many election precincts throughout the country, all of France can be counted in a matter of hours, in front of thousands of eyes.

I think you'll agree that the above system creates very little suspicion about the vote-counting procedure. Compare the trust gained by inviting many eyes, in the above example, with computerized vote-counting systems used in the USA right now:

• Computer programmers, who are not certified election officials, create a software system that will interpret and record the votes.

• The software program then takes its interpretation of the votes and adds them up inside a black box.

• The programming is done at a factory in Nebraska, or Vancouver, Canada, or Texas, or California, but citizens cannot look at the software.

• A copy said to be the program used in actual elections is then shipped to Huntsville, Alabama, where a testing facility examines it, but the tests are a secret and no one is allowed to interview the testing personnel.

• Then the secret code is sent to the secretary of state for each state that authorizes it, but no one really looks at the source code here. The secretary of state keeps the secret code locked in escrow.

• Election officials cannot view the vote recording or tallying because it happens inside a computer.

• Citizens can't see it, candidates can't check it and sometimes the results are wrong.

We don't use proper audit procedures and we don't pass the "many eyes" test, even if our elections are error-free (they are not) or honest (we can't count on that).

You cannot allow a system so fundamental to democracy to become opaque. Such a system will lose the trust of the people it must serve.

Following are suggestions for legislative reform to allow us to verify voting machine accuracy. Each of these suggestions deserves reasonable debate by a group that includes, at a minimum, people with accounting experience, people with programming experience and some ordinary citizens.

Suggestions:

One bill, as of the writing of this book, that holds promise is HR-2239 introduced by congressman Rush Holt. It needs stronger language to make the voter-verified paper ballot the legal representation of our vote, and beefed-up auditing procedures need to follow.

1) Require **voter-verified paper ballot** for all voting machines.

2) We favor a 100% audit of the paper ballots againt the machine count. There are ways to make this cheap and efficient. See *A Modest Proposal* later in the book.

3) If we decide not audit 100% of the precincts, we certainly need to develop robust auditing.

a) Require **spot-check audits** to compare voter-verified totals against voting machine totals. These totals should match exactly for touch screens, and very closely for optical scan machines.

b) **Discretionary audits**:

(1) Allow parties to select a percentage of precincts to audit.

(2) Allow election workers to audit any results deemed unusual.

(3) Allow the media to audit any precinct it deems of interest at their own expense.*

(4) Allow any citizen to audit any precinct, at their own expense.*

*If a significant error is found, the recount cost is born by the governemnt.

c) **Triggered audits** (hand counts)

(1) Insufficient randomness (e.g. three candidates get 18,181 votes; poll book shows voters arrived in alphabetical order; every Republican wins by exactly 3 % of the vote; the results of one machine vary widely from other machines at the same precinct)

(2) Breach of security (e.g. ballot box or memory cards misplaced, unusual time lag between poll closing and delivery of memory cards/ballot boxes to counting location)

(3) Digital signature of software doesn't match the certified version.

(4) Too close to call: Less than 1% spread

4) **Discrepancies** — Expand the audit if the difference between machine count and manual count is excessive, *whether or not the identified discrepancy would overturn the election*. For example, in a normal audit, if you were examining randomly pulled purchase orders, and discovered an anomaly, you would pull

a larger sample of purchase orders. Further discrepancies would trigger an audit of all purchase orders.

Voting machines which are found to have miscounted must be reported to the voting machine company, the elections board, the candidates, and the media.

Chapter 4 describes many potential ways to rig the black boxes. Election-tampering has been with us for 2,000 years, and is unlikely to go away just because we have entered the computer age.

When you look at paper ballot systems, you can see that many of the standard procedures they use were specifically designed to deter fraud. The same care needs to be given when setting up procedures for black box voting.

Isn't this time consuming?

If we are unwilling to make sure our voting machines count accurately, we shouldn't use them. The biggest objection to proper auditing is that it takes too much time, so some ideas follow for ways to run a relatively tamper-proof system efficiently and with minimal cost.

Implementation ideas

1) The simplest method is to have the touch screen systems print a paper ballot which is easily read by voters and election workers, but also contains a machine-readable bar code.

When the polls close, election workers can scan the bar code. This will take two poll workers approximately forty minutes to do an entire precinct. This gives us a 100% audit at the polling station

This is the cheapest, quickest and most secure method. Note, however, that the bar code scanner should not be from the same manufacturer as the voting machine.

2) Precinct counting: Bring in a second shift one hour before the polls close. After the normal day's work is done, let the tired folks go home. Second shift manually counts the ballots at the precinct level.

Limit the audit to national representative races, major state offices and a random selection of 1-5 propositions, judges and/or state committees, to start.

More exhaustive auditing would be optional depending on volunteer level.

3) Require **"vote audit" duty**, similar to jury duty. It can be during evenings and weekends only, so that it doesn't conflict with jobs. This might even get more people to start voting.

3) Pay poll workers to show up for one **extra day** for auditing duty.

The biggest objection to doing enough auditing to ensure system integrity is that it adds new things to do. Well, democracy is messy. The machines are new, and we certainly are willing to invest extra days to train poll workers for them. If the only way we can use machines safely is to audit their accuracy, let's put at least as much effort into that as we do into trying to learn how to use the machines.