Chapter 12
Black Box Voting

Ballot Tampering in the 21st Century

by Bev Harris

with

David Allen

Edited by

Lex Alexander

Cover Art by

Brad Guigar

12
A Modest Proposal

Well, are you ready for some action? The next chapter is called "Practical Activism," and it's full of ideas to help us take back our vote. But what, *exactly,* are we fighting for?

When I began writing Chapter 3 in June, I queried many in the voting activism community about what, exactly, we should *do* with a voter-verified paper ballot system once we get it. No one seemed quite sure, and the solutions for auditing in Chapter 3 came only after poking and prodding.

Now I have an even more fundamental question: What do we want?

The Help America Vote Act (HAVA) was supposed to bring reform, but seems to have made things worse. In a brave and prescient move, Congressman Rush Holt from New Jersey proposed HR 2239 to mandate voter-verified paper ballots, get rid of risky remote access tools, and require a spot check audit. His bill was a giant step in the right direction, but didn't adequately address auditing. The optical scan machines in San Luis Obispo County, California and Volusia County, Florida indicate that we don't have security under control, even when there is a paper ballot.

Emergency measures

Of the following three choices, which do you prefer and why?*

1) **Immediate moratorium on all machine voting**. Paper ballots *only,* counted by hand, until we can all agree on and implement a satisfactory system.

2) **Immediate addition of paper ballot option for any voter who requests one.** In other words, if you go to a polling place with touch screens, they must offer you a paper ballot if you request it, and they may not consider it a

*Go to www.BlackBoxVoting.org and click "forums" to discuss anything in this book.

"provisional ballot." (Almost all counties with touch screens also have optical scan machines, which are used to count paper ballots, so this should not be very difficult.) And while you're at it: Should we then require that no forecasts can be made on the winner until the paper ballots are counted?

3) **Get the machine count audited and ban systems that do not produce a voter-verified paper ballot.** By virtue of filling in or punching holes, that's what most of the current systems, with exception of DRE's or lever machines, provide, but they are not robustly audited, giving a false sense of security. If you choose this option, how exactly do you recommend beefing up the audit? See Chapter 3 for more input.

Voting machines aren't the only way to manipulate an election.

The topic of this book, and proposed reforms and activism, is how we cast, count and audit our vote. There are other battlegrounds, however, and all of them are important:

Biased redistricting: Voting districts are supposed to be evaluated every decade or so, but some political manipulators like to try redistricting whenever it looks advantageous, re-setting the boundaries in order to favor one party. There are ways to restructure the voting system to counteract this, though they are not the topic of this book.

Flawed or fraudulent voter registration: For some time now we've had dead citizens so enthused about social issues that they rise up and vote, and infirm nursing home residents who mysteriously register themselves even though they are comatose.

HAVA requires that we take our voter registration systems and put them into a statewide computerized database, brought to you by companies like Diebold and Election Systems & Software. Just as the scale of vote-counting risk increases with computerized voting machines based on secret software, the dimensions of voter registration fraud can be expected to explode under HAVA. Whereas in Florida in the 2000 election, we saw massive and inappropriate "felon purging" of registered voters who clearly had the right to vote, now we can expect charlatans to enter entire rosters of nursing home and graveyard residents into the new computerized voter registration system.

Then, when the "quaint" custom of physically checking a printout at the polling place is sidelined in favor of sleek new smartcards (manufactured by Diebold and Lockheed-Martin), hackers can have a go at electronically signing in everyone from the Happy Oak Cemetery.

Impeding access to the polls/ intimidation at the polling place: What exactly do minorities have to say that makes it so important to quell their voices? I say "*their* voices" with a struggle, because this business of sudden road construction around polling places, late poll openings, broken machines and not enough voting stations affects me and my own. And that's not all; political bullies have also been coming up with bright ideas like last-minute moving of the polling place (sometimes to the nearest *police station)* and posting "challengers" to question people trying to vote. These are vote suppression tactics that have been illegal for nearly a century, but they persist.

Retaliation after candidates are voted into office: Recalls are exciting, but are they good for democracy?

If you find that you like fighting for your right to vote, there's no reason to stop when we get the voting machine issue solved. There is plenty of work for everyone.

* * * * *

The activism chapter that comes next includes tactics that can be used for any election-manipulation issue, but we'll concentrate here on voting machine issues. What exactly are we asking for? I think we should cogitate before we agitate.

Here are three proposals. Which appeals to you most?

I. From Victoria Collier

Collier grew up discussing vote fraud around the dinner table. Her father, James Collier, and her uncle, Kenneth Collier, wrote *Votescam: The Stealing of America,*[1] published in 1992, the first hard-hitting book about high tech vote fraud. In 1970, Ken Collier ran for Congress against Claude Pepper in Dade County, Florida, picking up about 30% of the vote. As the electronic voting machine totals

weighed in, Ken Collier and campaign manager James Collier noticed that they suddenly lost 15 percentage points. They didn't get another vote for the rest of the night.

According to the Collier brothers, "[when they] compared the official vote results with a print-out of the vote projections broadcast by the TV networks on the final election night, they found that Channel 4 had projected with near perfect accuracy the results of 40 races with 250 candidates only 4 minutes after the polls closed. Channel 7 came even closer; at 9:31 pm, they projected the final vote total for a race at 96,499 votes. When the Colliers checked the "official" number . . . it was also 96,499."

"In hockey, they call that a hat trick," the Colliers write. "In politics, we call it a fix."

All Paper Ballots, All Hand-Counted:

"Listen, here's my idea," says Victoria Collier. "After the public touch-screen bonfire (we really need more community minded events, don't you think?), we should march to our secretary of state's office and demand the restoration of a hand-counted paper ballot system."

Collier recommends using properly designed, easy-to-use paper ballots and see-through boxes.

Whoever does it, Collier advocates that the count be done by hand, in public, video-taped, aired live on television, and the results posted on the precinct wall. If we count all ballots at the polling place on Election Day, it will be much harder to alter ballots.

She also recommends other security measures, to prevent ballot boxes from going missing on the way to the county elections office.

* * * * *

II. From Dr. Rebecca Mercuri

Who created the voter-verified balloting concept? Rebecca Mercuri did. She wrote of her design concept in a paper called **"**A Better Ballot Box,"[2] the

first, and probably the most widely accepted design for a hybrid electronic/paper ballot system.

The Mercuri Method

The Mercuri Method allows proprietary voting machines made by private manufacturers, but requires that they modify touch-screen or DRE machines to generate paper ballots. The system should record votes electronically, then print a paper ballot and display it behind a plastic or glass panel, which prevents the voter from removing it from the polling place, or accidentally mangling it so that it can't be easily read. The voter reviews the ballot. If it does not represent her choices, she calls an election official, who voids the ballot and she votes again. Once she approves the ballot, it drops into a ballot box for later tallying. This voter-verified paper ballot must be the definitive record of the vote.

In this system, the paper ballots can be tallied by running them through an optical scanner or hand counting them. The electronic count can be used to provide preliminary results, but the official result must come from the paper ballots.

If the ballots are configured correctly, they can be generically scanned. After the election, other groups could scan the ballots with their own equipment if so desired.

* * * * *

Words are important: "Paper ballot," never "receipt." A paper ballot is a legal record and substantial. A receipt is a small slip of paper we might stick in our pocket.

* * * * *

III. A Modest Proposal, From David Allen

Suppose we want to open source this, and take ownership of the voting system back into public hands. Here is a proposal for such a system.

The Tamper-Resistant Method

Allen's proposed system requires a paper ballot that uses anti-tampering features like those found in financial documents. The data in the system must be stored on non-eraseable media.

Everyone should be invited to watch the system being built, in the open rather than in secret.

Like Mercuri, Allen proposes a hybrid system, taking the best of the old paper ballot system with the best of the new computer systems.

Part of this system must be a real-time record of everything that happens on the voting machine: when the machine is turned on, when the machine is turned off, when someone enters a supervisor mode, when votes are cast. Each "key-stroke" of the election must be recorded.

"If we are going to use a 'black box' to vote on," says Allen, " then let's model it after the 'black box' found aboard airliners (even though they are actually orange, not black). After a plane crashes, the black box is fished from the wreckage and everything the crew did can be reconstructed.

The easiest way to do this with an electronic voting machine is with a "write-once" CD-ROM drive. At the start of the election, a CD-R is inserted into the machine and the drive sealed. The system is then powered up and everything that happens on the system is recorded to the CD. At the end of the day, the seal is broken, the disk removed, signed by the staff and any observers present and then sealed in a box for delivery to election HQ.

The computer prints a ballot, which we inspect, which is deposited into a secure ballot box. When the ballot is printed out, we now have an independent audit record, and the second part of a three-part auditing system. The third part of the system is the digital tally maintained on the voting machine's hard drive or memory card. All three should match:

1) Write-once CD-R

2) Voter-verified paper ballot

3) Hard drive or memory card

When the polls close, we tally the digital vote and compare it to the paper count. These two totals should balance. If they don't, there can only be three possible reasons:

1) You miscounted the paper ballots. (Recount them)

2) The hardware/software has malfunctioned. (Use the paper ballot as the official vote).

3) The paper or digital ballots have been tampered with.

Note that printing the tally before any transmission, and counting the paper ballots at the polling place, matching them to the electronic count, eliminates most of the risk in electronic transmission.

So, won't we be creating tons more work by having to hand count ballots?

A bar code can be printed along side each vote that a scanner can read, as long as the reader is generic and purchased from a source unrelated to the manufacturer of the voting machine. Ballots can thus be processed quickly at the precinct. Since the ballots are also readable by humans without requiring the aid of any device, it is easy to verify the accuracy of the scanner.

Do we really have to count all the paper ballots? Well, if we don't, we need a much more complicated set of audit rules (see Chapter 3); it is simpler, not costly, and not time consuming just to count them all.

Open source.

What is open-source software? It is software developed by a community of programmers in full view of the public in which all source code is open for inspection. The Linux operating system is an example of open-source development and is one of the most stable and secure computer operating systems on the planet.

Imagine the entire mechanism for counting your votes being conducted in the center of town with the public looking in from all sides. It is hard to do anything tricky with that kind of surveillance. Perhaps you are not a computer programmer, so putting the mechanism in the town square wouldn't help. Instead tens of thousands of programmers around the world are watching, but the effect is the same.

There is another reason to require open source programming: Suppose we have a system that counts the votes perfectly but, unbeknownst to us, secretly attaches our voter I.D. to our vote. With open examination of the source code, there is less opportunity for anyone to do something they shouldn't.

Once the code is developed, any company may use it and sell it to anyone they please. They just can't change the source code. They can bundle it with hardware, install it in precincts, teach poll workers to use it, and provide maintenance and support for the software and equipment. But, they must adhere to the inviolable commandment: Tamper not with the actual source code. It doesn't belong to you; it belongs to the taxpayer.

The software controlling the CD-R must be vetted and burned into a ROM chip (meaning it can't be erased or changed).

The question of hardware is trickier.

People are making all sorts of different equipment with varying features and levels of quality and support. The solution here is to have a body that specifies the minimum requirements for the hardware needed to run the software. As long as your hardware meets these specs, the local election boards can buy it. If it doesn't, they can't.

Several proposed solutions for open source electronic voting machines create code that is so simple that it can use inexpensive hardware, and even recycle old computers.

* * * * *

Open, public debate on our voting system is healthy and it is our right.

Several new Internet forums and activism groups are available, giving everyone ample opportunity to learn about solutions and discuss them. Add your voice now, and speak loudly, for if we don't insist on creating and getting general public agreement on our voting system, someone else will.

Chapter 12 footnotes

1 – *Votescam: The Stealing of America*, by James and Kenneth Collier; Victoria House Press, 1993

2 – Oct. 2002; IEEE Spectrum — "A Better Ballot Box: New electronic voting systems pose risks as well as solutions" by Rebecca Mercuri http://www.notablesoftware.com/Papers/1002evot.pdf