

January 7, 2008

OP-ED CONTRIBUTOR

A Paper Trail for Voting Machines

By WILLIAM POUNDSTONE

Los Angeles

PARANOIA over electronic voting is the new American consensus. The Democrats who will vote in the New Hampshire primary on Tuesday aren't worried that Hillary Clinton will steal the election from Barack Obama or John Edwards, but a good chunk of them would probably confess to dark fears about a Republican plot in November, even if Karl Rove won't be involved.

Last month, Colorado's secretary of state, Mike Coffman, a Republican, decertified the state's electronic voting machines, after the alarming finding that one model could be disabled with a magnet and others were scandalously inaccurate. He left voters to draw their own conclusions about what this meant for the state's most recent elections. The California secretary of state, Debra Bowen, a Democrat, took office last year after running on a don't-trust-electronic-voting platform, and in August she pulled the plug on the state's voting machines.

But what other options are there? Paper ballots aren't perfect. Ballot boxes can be stuffed or lost. Indeed, because of Florida's paper-ballot mess in 2000, electronic voting is probably here to stay.

Fortunately, there is an elegant solution that lets us use modern technology while assuaging the growing fears about voter fraud. Ronald L. Rivest, a Massachusetts Institute of Technology computer scientist, and Warren D. Smith, a mathematician and voting reform advocate, have proposed an ingenious method that would combine paper ballots and a Web site to achieve greater ballot security than is possible with paper or software alone.

Their basic idea is to allow each voter to take home a photocopy of a randomly selected ballot cast by someone else.

The scheme is low-tech. Paper ballots would be tallied by optical scanners or even by hand. The results would be then posted on a Web site. Using a serial number assigned to each ballot, voters could check the site to make sure that their random ballots were posted and had not been altered or misread.

To discourage vote buying, voters would not receive copies of their own ballots. My receipt would be someone else's ballot, so I would have no way of proving to a bribe-wielding politician whom I voted for. (There are no voter names on secret ballots, of course, so the random receipts would not compromise the privacy of the voting booth.)

Yet another opportunity for fraud, perhaps more likely than outright vote buying, would be created if voters were given paper records of their own ballots. Many voters would ditch their receipts in the first trash can they see. Then, crooked election workers could retrieve the discarded receipts and change the corresponding

electronic votes, confident that there would be no evidence of their fraud.

But under the system proposed by Professor Rivest and Dr. Smith, should corrupt poll workers “forget” to count some ballots, people would notice and complain. And because the receipts are copies of ballots chosen at random each time, a few ballots would be copied twice or more. Finding a discarded receipt would not guarantee that it is “safe” to change the corresponding vote — there might be other copies of the same ballot floating around, and some watchful citizen might be checking them.

The Web site would also publish the names of everyone who voted. This would prevent someone from undetectably adding fake votes from names copied off, say, tombstones.

Perhaps best of all, because a public Web site would post the complete information from every ballot, anyone could check that every single vote has been counted accurately.

Too much trouble, you say? Don’t bother, then. All that matters is that some concerned citizens check. The news media, the political parties, activists and bloggers would be checking so that the rest of us don’t have to. Indeed, Professor Rivest and Dr. Smith demonstrate mathematically that it takes only a tiny number of people checking the Web site to catch any substantial fraud with near certainty. For instance, to have 95 percent assurance of detecting a fraud involving 6 percent of ballots, only 50 voters would have to check, and this is true no matter how large the electorate. If the margin of victory is less than 6 percent, then more people would surely check.

The virtue of the system is its simplicity. The only technology that would be required is a Web site and a scanning printer that could produce a copy of a random ballot for each voter at the press of a button. That wouldn’t be hard to devise.

As YouTube demonstrates, the Internet is a leveling force, allowing people to assume roles formerly left to professionals. The Rivest-Smith scheme would make ensuring fair elections everyone’s business.

William Poundstone is the author of the forthcoming “Gaming the Vote: Why Elections Aren’t Fair (and What We Can Do About It).”

[Copyright 2008 The New York Times Company](#)

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)