

# ONLINE JOURNAL™

www.onlinejournal.com

## Computerized voting systems cannot be made secure

By Bev Conover

Online Journal Editor & Publisher

October 20, 2003—If Microsoft can't make its operating systems, browser and email clients secure, what makes anyone think computerized voting systems can be made secure?

Whether you love, hate or are indifferent to Microsoft, think about this: Microsoft, with all its money and skilled programmers, has to keep scrambling to plug holes in its software. The same might be true of Apple or any of the others if they had the same market share as Microsoft.

Yet, some 37 states, with more about to take the plunge, have opted for the worst of all computerized voting systems: touch screens that leave no paper trail. What were these legislators thinking? Were they thinking? Or are they just a bunch of techno-dummies who fell prey to the charms of the makers of this equipment—charms that may have included possible campaign donations? Whatever, they have wittingly or unwittingly sold the people out.

Nothing in this world is foolproof or can it be made fail-safe. Anything one person devises, another can find a way around it. That's the nature of the world. Total security is a myth. All we can have is degrees of security, such as locking the doors to our houses when we leave them or at night. But those locks and even those security systems so many have installed, while they may slow down and even deter an amateur burglar, will not keep a professional burglar out.

Remember The Club that device you put on the steering wheel of your vehicle to thwart car thieves? While it may have warded off the amateur, the professional simply either cut through or removed the steering wheel and made off with the vehicle.

If such simple devices offer such little security, think about computers and software with millions upon millions of lines of code and the difficulty, if not impossibility, of closing every door, so to speak, to keep someone from messing with that code or planting something that does nasty things to your computer. Yes, you can install anti-virus software and firewalls, but they only offer a degree of protection, that is, if you keep them updated. Think how much time, money and effort is spent by the anti-virus makers in trying to keep up with nasty people who write nasty codes. Moreover, some of these nasty people can even remotely install software on your computer that allows them to use it for nefarious purposes, in addition to remotely installing spyware and keyloggers to keep tabs on everything you do. Yes, if you're a bit of a nerd you can install software that will tell you that someone has installed these things on your computer or send you into a panic over innocent things, such as legitimate cookies, because such software is far from perfect.

But despite the hacking, the viruses, the worms, the Trojan horses that have affected millions upon millions of computers—corporate, government and private—the makers of computerized voting systems and the legislators who support them want you to believe your vote is secure. They want you to overlook the proven holes in these systems, much less consider that the vote you cast may not be the vote that is recorded. The last thing they want is a verifiable paper trail that would be counted and compared to the machine tally.

Even the League of Women Voters (LWV) showed its colors by posting to its website the [Leadership Conference on Civil Rights' \(LCCR\) Election Reform Policy Analysis](#), which opposes "voter-verified paper trails."

When it comes to vote-rigging the LWV was on the suspect list of [VoteScam](#) authors James M. and Kenneth F. Collier. The Colliers, who spent 25 years of their lives tracking election theft, pointed their fingers at the LWV for allegedly being involved in nefarious goings on in Miami-Dade County, FL, and Cincinnati, Ohio, in addition to its work as election night field representatives for the highly secretive News Election Service (NES)—the private media consortium (ABC, CBS, NBC, CNN, The New York Times, the Washington Post, AP Wire Service and others) that brought you the election returns—which morphed into Voter News Service.

In its July 9 analysis, which also is available on the [Civil Rights Coalition for the 21<sup>st</sup> Century's site](#), the LCCR refers to the touch screen systems as *direct recording electronic* (DRE) voting machines, noting “Some people, however, have attacked these newer machines, claiming that they are dangerously prone to manipulation, and that hardware or software failures are especially susceptible to resulting in lost votes. Some have even gone as far as to suggest that new machines are being used as part of a conspiracy to rig elections around the country.”

In dismissing the need for verifiable paper trails, the LCCR said, “The integrity and reliability of the voting process is of the utmost importance, and the creation of electronic records that can be used for audits and recounts is essential. Technology that allows voters to check their ballots before casting them, as is required by HAVA, is also very important. However, many of the concerns that have been raised over the reliability and security of DREs are overstated or unwarranted. Furthermore, while calls for the production of a *voter-verified individual-ballot paper trail* by DREs may be well-intended, such a step would lead to a wide range of negative consequences.”

And what are those negative consequences in the LCCR’s estimation? Well, somehow they would rob people with disabilities of a secret ballot. Huh? But having the machine read back to them their vote—assuming that’s audible—preserves the secrecy of their ballots. Double huh?

Excuse Number 2: There are no DREs that “produce a voter verified paper trail in wide use anywhere in the world. In a recent October 2002 trial of this new technology in Sacramento, CA, for example, printers jammed, and the ballots had to be handled with ‘many creative tools that were on hand . . . such as a windshield wiper or a back scratcher.’ Such breakdowns require entire machines be taken out for service, taxing poll workers and creating long lines at the polls. Vendors are working to create new DREs that produce voter verified paper ballots that meet secrecy and security concerns, but these new machines have mostly not been certified by testing agencies and have not been tested in the field.” So why rush into the technology until it can spit out paper trails just like an ATM or the credit card readers that have become popular at gas stations?

Excuse Number 3: “A piece of paper that shows the voter what they are voting for does not necessarily ensure a secure vote, because assuming a DRE can be rigged, what a paper receipt shows and what the machine counts could *still* be two different things. A better way to ensure accuracy, in addition to rigorous pre- and post-election testing, is to randomly take machines offline during election day and vote on them numerous times to ensure that votes are being counted correctly, a procedure known as parallel testing.” Oh yeah, take the machines offline during the day for “parallel rigging.” Isn’t that a super idea?

And if you thought Excuse Number 3 was a doozy, here is Excuse No. 4: “Producing a paper record creates privacy concerns, as strong security measures would need to be taken to ensure that voters could not take the paper receipts with them upon leaving the polls—opening the door to the sale or even coercion of votes—or that poll workers or elections officials could not violate the sanctity of secret ballots. Keeping a voter’s vote secret is critical to a free and fair democracy.”

In 1892, mechanical voting machines were introduced in US elections. Punchcards came on the scene in the mid-1960s, followed by optical scanners—both systems using computers to tally the votes. By 1996, fewer than 2 percent were still using paper ballots and pencils to cast their votes. Think how many paper ballots and pencils could be purchased for the billions being spent on touch screen systems, in addition to paying poll workers a decent hourly wage for the 12, 13 or more hours they put in to oversee elections

and tally paper ballots. Yes, it is possible with paper ballots to steal a local or even a district election, but it's much harder to steal a whole state's election.

The most important thing to any person in any society that is based on democratic principles is his or her vote and the right to have that vote counted as he or she cast it. As Americans that is more important to us than the constitution or the flag if we are to regain our country, because if our votes are stolen, the rest doesn't matter.

Too many Americans do not understand how precious their votes are. They have been brainwashed into believing a single vote doesn't matter. Well, it matters a lot. Despite nonsense to the contrary, no person's vote counts more or less than any other person's vote. It's one person, one vote. It is a travesty to allow the means by which we vote to be controlled by private corporations.

Yes, the politicians and the corporations that control them and the news media have done all in their power to drive people away from the polls, while feigning shock at the shrinking voter turnout. They have done a good job in turning people off to the political process. The corporations are one step short of achieving America Inc. If they get away with forcing their easily rigged, non-verifiable, and impossible to secure computer touch screens on us, the corporatization of America will be complete.

Copyright © 1998–2003 Online Journal™. All rights reserved.