

**There's No Place Like Home: The State Board of Elections Struggles to do the Impossible when the Possible and Best Solution for Transparent, Safe, Reliable Elections is Right Here:
Plan "L"- Our Lever Voting System**

Open letter to New York's State Board of Elections Commissioners:

I watched the October 3, 2008 meeting of New York's State Board of Elections (SBoE). Commissioner Peterson hit the proverbial nail on the head. **"If you have something that works and something that doesn't work, I vote for the thing that works."** Our lever voting system works to provide New Yorkers with trustworthy election results. Software-driven optical scanners and DREs can never satisfy the requirements of a democracy because the vote counting is concealed from the public, the very people who have to see and know that their votes are being counted as cast.

The Thing That Doesn't Work- Software-driven Voting Machines

The thing that doesn't work are the computerized voting machines which the federal government doled out 4 billion of our tax dollars to be funneled back to a few vendors and the states all jumped and now they're stuck. The evidence of failed machines is overwhelming. Commissioner Aquila is to be commended for pointing out the thousands of reports of failed and broken voting machines. At the June 19, 2008 meeting Commissioner Kellner summarized the problem accurately: "[T]he voting industry sells crap. And that's the problem." *

However shoddily made machines is not the only problem that is clearly frustrating all the State Board of Election Commissioners. Even if they didn't break down regularly, these software-driven machines cannot be made secure enough for a democratic elections, as demonstrated by dozens of reports from computer scientists around the nation (http://sites.google.com/site/remediaetc/home/documents/Scientific_Studies_7-20-08.pdf?attredirects=0). The standards the federal government has permitted the states to use in running elections on these vulnerable-to-massive-tampering machines is inadequate to secure election results and inferior to the standards New York has set for New Yorkers over the past two centuries. In New York we have had nothing more than the standards of democracy: our courts and successive legislatures have insisted on security, reliability and transparency. We have historically required that all known opportunities for fraud be prevented. In our lever voting system we have an electoral system that is observable and designed to detect, expose and prevent tampering. And it works!

But the computerized machines New York is earnestly testing will never be capable of being certified as suitable to "ensure the integrity and security of the voting machine or system" (Election Law 7-202 (1)(r)) because that is impossible. This is the assessment of the National Institute of Standards and Technology (NIST), the experts who advise the US Election Assistance Commission on the writing of federal voting system standards to which NY voluntarily adheres. In a November, 2006 report, NIST found that, "...testing to high degrees of security and reliability is from a practical perspective not possible." **

Below, I have included relevant excerpts from just a few of the dozens of independent computer scientists, each corroborating the other's findings that these voting machines are incapable of providing security and reliability because software is vulnerable to undetectable and therefore unpreventable tampering. Distilling the evidence this way perhaps explains why twice during the meeting Commissioner Peterson used the expression 'boggles the mind' referring to the expectation of the federal government that we should find a way to certify these machines as safe to use.

The Thing That Does Work - Our Lever Voting Machines

Returning to Commissioner Peterson's nail hitting quote above, what does work is our lever voting system. Not only has it proved itself in a century of service but with proper maintenance it will continue to do so for another century. Bryan Pfaffenberger, a professor at the University of Virginia who received a Scholar's Award from the National Science Foundation to study the history of lever voting machines, concluded:

"In New York, the people, in their wisdom, created a system of election administration AND a technology that solved the characteristic problems of American elections; to abandon lever machines for new technologies that will not gain voter confidence and, at the same time, re-introduce paper audit trails or paper ballots which have long proven to be prone to election fraud, amounts in my opinion to a potentially disastrous mistake." ***

Professor Pfaffenberger describes the lever voting machines as one of the greatest achievements of American inventive genius, explaining how New York was the proud beginning of this eminent technology. It is fitting that we not allow New York to be the state that sounds the death knell for this superior technology.

Our Lever Voting System is HAVA-compliant

When the State Legislature enacted ERMA in 2005 most of the scientific

reports referenced herein, revealing these machines' inability to securely count our votes, had not yet come out. HAVA required that disabled citizens be able to vote independently, the single federal requirement our levers couldn't comply with. But since we've installed ballot marking devices (BMDs) in every poll site for 2008 we have overcome that federal impediment and thus our lever voting system, combined with the BMDs, now complies with HAVA. That is the "Plan B" Commissioner Peterson called for, anticipating that another couple of months of testing would leave us "sucking our thumbs" and result in having these "machines jammed down our throats" unless we had a Plan B. Since Plan B already refers to something specific at the SBoE, let's call this the Plan L- for our Levers. Plan L will prevent the shoddily made, unsecurable computerized machines from being jammed down our throats.

I have spoken to many of the county election commissioners, all of whom would choose to stay on our levers but for NY's Legislature enactment of the Election Reform and Modernization Act (ERMA). But the Legislature left it to the State Board of Elections to replace our levers by certifying software-driven voting machines if it could. With all due respect, they can't. Consistent with the experience of the valiant and frustrating efforts of the SBoE, these machines have been thoroughly examined by dozens of independent computer scientists and repeatedly exposed for their vulnerability to unprotectable and massive tampering. New York can continue testing, costing taxpayers excessive time and money, but testing will only reveal what has already been proven-- which is that these machines cannot legitimately be certified as safe for use. Indeed, certifying such machines as secure or reliable would contradict the findings of every one of the scientific reports that have come out in the past few years.

We are the only state in the nation left with a secure, reliable, observable, demonstrably accurate voting system. The State Board of Elections is the agency entrusted with ensuring that the machines and systems new Yorkers are required to vote on can produce trustworthy results. We are fortunate that we still have such a system and aren't forced to go the way of the rest of the nation suffering with 'crappy' and theft-enabling computers.

On behalf of the residents of New York, we implore you to follow your conscience, stop and consider what you have already accurately perceived and look at the overwhelming evidence. **Vote for the machine that works. Vote Plan L. Save our lever voting system.**

Thank you

Andrea T. Novick, Esq.

* See EYES WIDE SHUT: New Yorkers Struggle for the Soul of Democracy, <http://www.opednews.com/articles/EYES-WIDE-SHUT--New-Yorker-by-andi-novick-080707-74.html>

** "[E]xperience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible."

- National Institute of Standards and Technology (NIST). Requiring Software Independence in Voluntary Voting Systems Guidelines 2007: Security and Transparency Subcommittee Recommendations for the Technical Guidelines Development Committee. November, 2006.

Excerpts from the reports of computer scientists who have examined these software-driven voting machines

1. In Dec. 2007 the state of Ohio tested all of its voting machines and found, "All of the studied systems possess critical security failures that render their technical controls insufficient to guarantee a trustworthy election." -- Ohio Secretary of State, Project EVEREST Report of Findings, December 14, 2007

In a recent interview Ohio's Secretary of State Jennifer Brunner was asked about the state's EVEREST evaluation of the voting machines used in Ohio (<http://www.bradblog.com/?p=6483>):

"When I finally saw the results of our [EVEREST] tests, I thought I was going to throw up. I didn't think it would be that bad. And it was - it was awful. I looked at it on a Saturday morning, and that night I went to bed and woke up [just before 4:00 on] Sunday morning going, "Oh my God." I never wake up on the weekends - trust me."

When discussing its study, Project EVEREST researchers reported:

"The second key finding of the review was the apparent vulnerability of the system to malware infection and manipulation. If a properly skilled and resourced attacker can gain access to any of several components in the system at any time during their life-cycle, there exists a large possibility that they could implement malicious programming (malware) into the system with little chance of detection. Once the malware was in place on the system, it could perform a variety of tampering and could likely spread from component to component throughout the system.

"The ability of malware to affect the integrity and availability of the elections process is profound and disturbing, but the lack of capability to detect and report potential malware attacks against the system makes it the single largest threat."

-- Ohio Secretary of State. Project EVEREST: ES&S System MicroSolved, Inc. Executive Summary Report. n.d. (December 2007).

2. In July, 2007 the state of California undertook a top to bottom review of all voting machines in use in the state and found: "An attack could plausibly be accomplished by a single skilled individual with temporary access to a single voting machine. The damage could be extensive – malicious code could spread to every voting machine in polling places and to county election servers."

-- Calandrino, Joseph A., Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller. Source Code Review of the Diebold Voting System. University of California, Berkeley under contract to the California Secretary of State, Top to Bottom Review, July 20, 2007 commissioned by the Secretary of State.

3. "The current certification process may have been appropriate when a 900 lb lever voting machine was deployed. The machine could be tested every which way, and if it met the criteria, it could be certified because it was not likely to change. But software is different. The software lifecycle is dynamic...[Y]ou cannot certify an electronic voting machine the way you certify a lever machine.... [W]e absolutely expect that vulnerabilities will be discovered all the time....

"Software is designed to be upgraded, and patch management systems are the norm. A certification system that requires freezing a version in stone is doomed to failure because of the inherent nature of software."

-- Rubin, Avi (Professor of Computer Science at Johns Hopkins University). Secretary Bowen's Clever Insight. Avi Rubin's Blog, August 7, 2007.

4. [W]hile 'logic-and-accuracy testing' can sometimes detect flaws, it will never be comprehensive; important flaws will always escape any amount of testing."

-- Wallach, Dan S. Testimony to National Institute of Standards and Technology and Election Assistance Commission Technical Guidelines Development Committee, September 20, 2004.

"This is a classic computer security problem. Whoever gets into the machine first wins. So if the Trojan horse software is in there first, you ask it to test itself -- it will always lie to you and tell you everything is fine. And no matter what testing code you try to add after the fact, it's too late. It can now create a world where the testing software can't tell that the machine has been compromised, even though it has...."

-- Dan Wallach, Rice University computer security expert has examined electronic voting systems since 2001, and has testified about voting security issues before government bodies in the U.S., Mexico, and the European Union. Quote from Peering through the chinks in the armor of high-tech elections, May 27, 2007

5. Florida's Department of State commissioned a report in 2007 which found, "Flaws in the Optical Scan software enable an unofficial memory card to be inserted into an active terminal. Such a card can be preprogrammed to swap the electronically tabulated votes for two candidates, reroute all of a candidate's votes to a different candidate, or tabulate votes for several candidates of choice toward a different candidate.

-- Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Waalega, Evan Hollander, and Michael Gerke. Software Review and Security Analysis of the Diebold Voting Machine Software. Florida Dept. of State: Florida State University, Security and Assurance in Information Technology Laboratory, July 27, 2007.

6. "There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots."

-- California Voting Systems Technology Assessment Advisory Board (VSTAAB), Security Analysis of the Diebold AccuBasic Interpreter, February 14, 2006

7. In 2003, a report for Congress found: "[T]he growing use of information technology in elections ... provides the opportunity for new kinds of attacks, from new kinds of attackers."

And, later, "New and more ingenious kinds of malware are constantly being invented and used. There are now tens of thousands of known viruses, and the sophistication of tools used to develop and use new ones has increased.

"Malware in a voting system could be designed to operate in very subtle

ways, for example, dropping or changing votes in a seemingly random way to make detection more difficult. Malware can also be designed to be adaptive - changing what it does depending on the direction of the tally. It could also potentially be inserted at any of a number of different stages in the development and implementation process - from the precinct all the way back to initial manufacture - and lie in wait for the appropriate moment."

-- Fischer, Eric A. CRS Report for Congress: Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. Congressional Research Service, November 4, 2003.

*****From Professor Pfaffenberger**

(and see recent article published by Dr. Pfaffenberger entitled, Making Every Ballot Count, <http://oscar.virginia.edu/explorations/x14206.xml>)

I've received a Scholar's Award from the National Science Foundation to study the history of lever voting machines, a subject that has never been studied by a scholar with professional training in the history of technology (or in any other discipline, for that matter). I am currently writing a book tentatively titled *Machining the Vote*, which covers the history of lever machines from their invention in 1888 to the bankruptcy of the leading manufacturer, Automatic Voting Corporation, in 1983. Highlights of my findings:

1. In my analysis, the lever machine deserves recognition as one of the most astonishing achievements of American technological genius, a fact that is reflected in their continued competitiveness against recent voting technologies in every accepted performance measure. With as many as 28,000 parts, their mechanisms reflect an agonizingly difficult period of development, spanning more than twenty years (1888-1919) in which interlocking mechanisms had to be developed that were capable of dealing with the enormous complexity and variety of American elections. The result was a machine that captures in its immutable mechanical operations the voting rules that the American people, in their wisdom, developed in order to capture the will of the people.

The mind balks, perhaps, at the suggestion that a century-old technology might be the equal of today's best technologies -- or even superior! -- but the fact is that the lever machine is not alone. U.S. freight railroads continue to use electromechanical signaling systems that were, coincidentally, developed during almost exactly the same frame (1890s-1920). There is no sense of urgency to replace them. Their reliability has been proven in a

century of service. They are perfectly adapted to the conditions of American railroading. They are easily understood and maintained by technicians with modest educational backgrounds.

2. Time and again, as I mentioned earlier, lever machines won the confidence of election officials and the public, even when doubts were expressed. I'd enjoy sharing the New York story with the commissioners. By 1925, most of upstate New York was voting on lever machines quite happily, but New York City - led by Tammany Hall Democrats -- resisted. New York's first activist Attorney General, Albert Ottinger, vowed to impose lever machines on the city whether Tammany liked it or not -- and by 1926, they were used throughout much of the city. The 1926 election proved to Republicans that, contrary to their suspicions, the New York City Board of Elections had been running fairly clean elections -- the much anticipated, 50,000 vote payoff did not materialize. At the same time, Democrats realized that the machines did not amount to a Republican plot, since Democrats won squeaker elections in districts that normally lean Republican. Suddenly, the voting machine controversy in New York City ended abruptly. Election officials elsewhere had been watching this drama and, when it reached what all agreed was a happy conclusion, voting machine adoption took off throughout the country. Throughout all the years of the Depression, even, the voting machine business was profitable and AVC paid dividends to shareholders. By 1960, about 60 percent of the voters in the U.S. cast their ballots on the machines. In that year, of course, Kennedy narrowly defeated Nixon, leaving Republicans convinced that corrupt Democratic election officials in Chicago and Texas were to blame. In Chicago, the controversy was almost entirely focused on the precincts where paper ballots were still in use. In contrast, where lever machines were used, there were few irregularities. Had lever machines been in use throughout Chicago, it is possible that our nation would have survived the 1960 without generating a politics of payback that continues to this day.

3. Although lever machines do not produce an independent audit trail, this is -- as software engineers say -- a feature, not a bug. In the 1880s and 1890s, paper ballots emerged as the locus par excellence of election fraud; lever machines were expressly designed to take the human element out of every aspect of the vote recording and counting process in order to eliminate fraud that was gravely undermining Americans' confidence in their democracy. It is quite astonishing to realize that, while the lever machine was under development, inventors came up with just about every voting machine concept that has since been realized, including precinct-scan punchcard technologies, ballot printing machines, and even electromechanical systems that can be seen as predecessors of computerized technologies. All of these technologies produced paper

records, however, and all were flatly rejected, both by voters and election officials, as letting the possibility of fraud in through the back door. Today, there are widespread calls to bring paper back into the picture, but the reason is that people do not trust the machines.

Having studied the history, I strongly believe that there would be no such call for paper if the ugly history of fraudulent practices enabled by paper ballots were known -- unfortunately, the American people have forgotten the lessons they learned a century ago, and I greatly fear that we will have to repeat them in order to learn them again. The truth of the matter is that our American election system, in contrast, to the election administration systems of most advanced democracies, is inordinately decentralized, less than professionally administered in many instances, and politicized. In New York, the people, in their wisdom, created a system of election administration AND a technology that solved the characteristic problems of American elections; to abandon lever machines for new technologies that will not gain voter confidence and, at the same time, re-introduce paper audit trails or paper ballots which have long proven to be prone to election fraud, amounts in my opinion to a potentially disastrous mistake.

Bryan Pfaffenberger
Department of Science, Technology, & Society
University of Virginia

Brief bio about Professor Pfaffenberger:

An anthropologist by training (Ph.D.: University of California, Berkeley, 1977), Bryan Pfaffenberger has been committed to science and technology studies for more than two decades and has received international recognition for his scholarly work in STS. He is the winner of the Albert Payson Usher prize (1989) for this essay, "The Harsh Facts of Hydraulics: Technology and Society in Sri Lanka's Colonization Schemes" (Technology and Culture) and the American Society for Information Science's Book of the Year award for Democratizing Information (G..K. Hall, 1989). In addition, he continues to work in the anthropology of technology, recently described by a leading anthropologist as the first successful new subfield of anthropology to have been created in a quarter of a century. His work, including a key 1994 essay titled "The Social Anthropology of Technology" (Annual Review of Anthropology), helped both to create the new subfield and provide it with rich theoretical tools. Pfaffenberger's current interests focus on the social analysis of computing, including electronic voting and the impact of a rapidly expanding U.S. intellectual property regime on engineering, science, and technology.