Memo II: To The Honorable Eliot Spitzer, The State Board of Elections, New York State Legislature
From: Andrea Novick , Esq.
Date: July 24, 2007
Re: Alternative Voting Systems that are HAVA-compliant, NYS-compliant and Democracy-compliant

The Help America Vote Act (HAVA) of 2002 saw states rush to purchase electronic voting machines allegedly as the solution to the problem in Florida 2000 (which problem of how to discern voter intent was never solved by these new machines, but only made worse). The results have been nothing short of disastrous, given the high incidence of machine breakdowns, rigging, vulnerability to fraud, overall shoddy performance of these private computerized voting machines.[1] The vulnerability of these electronic voting machines have been repeatedly demonstrated and are widely known to be security risks so serious they can undermine an entire state or national election. [2] However the voting vendors, *choosing* to use proprietary software, continue to conceal these serious problems, enabled in part by the secrecy surrounding their software.

Having refrained from the haste of the rest of the country New York is now in a unique position not only to avoid repeating other states' mistakes, but to learn from them. Much of the resistance to creating viable, secure voting systems has had to do with the fact that the states have already spent billions of dollars on these machines and feel committed to that investment. If you can't afford to toss your Pinto, having discovered it will blow up on impact, you're stuck with adding the "improvements" only Ford offers in the hopes of making your car less vulnerable. But New York isn't saddled with a Pinto. We can make a choice based on what will best serve the needs of a democracy; a consideration that was overlooked by the others in their eagerness to embrace these machines.

New York has not yet committed millions towards these too-unsafe-at-any-need voting machines. We can still stop and consider that the constitutionally protected right to vote includes:

> *securing to all citizens...**the right freely to cast their ballots** for offices to be filled by election and **the right to have those ballots**....**received and fairly counted**. Legislation which fails in such respects and prevents the full exercise of the right as secured by the Constitution is invalid*." (emphasis supplied)
>
> *Hopper v Britt*, 203 NY 144, 151 (Court of Appeals, 1911).

To the extent New York's Election Law is construed to circumvent our fundamental and inalienable right, thereby preventing its full exercise, it cannot lawfully justify the purchase of equipment that could potentially disenfranchise millions by virtue of these machines' unacceptably high security vulnerabilities and other documented failures.

Democratic Elections must Be Open, Transparent and Accountable to the Public

Elections are the means by which citizens in the United States assert their right to be independent by choosing those who would represent them. This mechanism for self-governance, intended to protect Americans from a return to tyrannical rule, was set forth in the Declaration of Independence, described therein not merely as a right, but as a duty. **Accordingly the people are ultimately responsible for the government and therefore cannot surrender control of the process of their elections: not to the government nor to any private corporations, particularly ones asserting secret proprietary rights to the very information that would provide knowledge about how their computers are processing our elections and counting our votes.**

Surely the public's vital interest in transparency and accountability trumps a private corporation's claim to conceal the critical information citizens must have to know their elections are fair and honest. There was a time, not too long ago, when such a statement would have seemed superfluous. But when 49 states have permitted private interests to run the people's elections on private computers, insisting on trade secrecy privileges to conceal from the public all information about the means by which we elect those of whom we expect transparency and accountability, we must state the obvious: We must demand transparency and accountability of our government. We in New York are fortunate to have not made the mistake of contracting with vendors who oppose transparency and to have a Governor who has embraced a vision for increased government transparency.

People can monitor their elections only when the process is visible: when they can observe that election workers are following procedure and that the ballots are properly counted. This is in direct contrast to the invisibility of computers that now perform most of the functions previously undertaken by trained poll workers. Not only do computers deprive citizens of meaningfully engaging in oversight and scrutiny of their elections, but the private vendors selling voting systems, assert an unestablished extension of intellectual property rights to include trade secret protection over the source code: the very information which directs the computer as to how to run the election and how to count the ballots! Had the nation not rushed to embrace the privatization of its elections I am convinced any respectable court, if given the opportunity in advance of the millions now invested, would have readily recognized that private vendors with their secret proprietary software can have no role in a free society.

New York, the only state which has not privatized its elections, must be a beacon for the rest of the nation. We are the last state. It is up to us to resist what is clearly antithetical to the very notion of democratic elections. As the only state not to have succumbed, it has become necessary to act boldly and alone in order to preserve the freedom this nation has enjoyed for over 200 years.

> *"A people may prefer a free government, but if, from indolence, or carelessness, or cowardice, or want of public spirit, they are unequal to the exertions necessary for preserving it; if they will not fight for it when it is directly attacked; if they can be deluded by the artifices used to cheat them out of it; if by momentary discouragement, or temporary panic, or a fit of enthusiasm for an individual, they can be induced to lay their liberties at the feet even of a great man, or trust him with powers which enable him to subvert their institutions; in all these cases they are more or less unfit for liberty: and though it may be for their good to have had it even for a short time, they are unlikely long to enjoy it."* -- John Stuart Mill

Historically, election workers ran elections and counted the ballots by hand, observed by the public whose responsibility it was to watch (literally still called "watchers" throughout the NYS's Election Law). By watching, diverse citizens could observe that all procedures established to insure the integrity of the electoral process were abided. This was done, as it should be, in the open so that any errors or problems could be immediately identified and responded to. Election administration has historically recognized that the best way to demonstrate the integrity of an election is by inviting public scrutiny. The only way the public can have the necessary oversight is for every aspect of the process to be made open and transparent; particularly the counting of the ballots. Secrecy never had and never should have a place in our elections.

As the nation has moved towards the use of machines in our elections, we have lost much of the transparency essential for checks and balances. We have lost the ability to observe and with that the accountability indispensable to the functioning of democracy. This is a national crisis. Fundamental to the long-term survival of a democratic society is the appreciation that government derives its legitimacy from elections the people trust. We cannot trust what we cannot see; and faith has no place in our secular republic. Only a citizen-owned process can legitimize government through the consent of the governed.

For these reasons I have been advocating and continue to believe the best option for democratic elections remains a full manual hand count of all paper ballots: only then can regular citizens know, without having to rely on experts or government officials, how their votes were processed and counted. I recognize New York's lever machines were a response to the corruption of 19th century hand counting practices, but given proper protocols, and particularly today in the age of the surveillance camera, hand counting is the most open, observable and hence accountable means we have to preserve the integrity of our elections[3]. The lever machines, in their time, may have had success in combating the inevitable fraud that is always a potential in elections, but New York's current law has seen fit to outlaw lever machines. However moving to electronic voting machines without sufficient means of achieving transparency and oversight will deliver our elections into the hands of those looking to rig the election in a way never before possible. Both the massive scale of the fraud as well as the ability of this theft to be committed by a single individual is made possible for the first time in history by electronic voting technologies.[4]

In light of the voting machine certification testing timetable New York is proceeding on and the current resistance within government to prepare citizens to hand count their ballots, I see no way to effectuate that hand count protocol before New York too starts spending money to privatize its elections. Lacking the political will and leadership to make hand counting a reality for the 2008 election it will take a ground swell from the people. Ground swells take more time than we have to prevent the privatization of our electoral system. For this reason I have been exploring the use of open source software programming for managing elections as an alternative to the confidential proprietary software systems offered by the major vendors. As a result of my investigation, I remain convinced that a full citizen hand count of paper ballots with proper protocols to avoid the problems New York was experiencing at the turn of the last century, remains the best means of fulfilling our duty as citizens of this republic. However, if New York insists on purchasing machines to assist in the counting of our votes, it can only do so using publicly owned, non-privatized, open source software optical scanners.

As I set forth in my memo I*, The voting vendors scheduled for certification testing are ineligible to contract with New York,* not only is New York enjoined from contracting with the major vendors since none of them satisfy the ethical integrity and performance standards set forth in our laws, but privately controlled proprietary voting systems undermine our laws, our Constitution and our ability to have honest and fair elections. A voting vendor that insists proprietary rights to conceal the very information required by the public to know that its representatives have been fairly elected, cannot be permitted to participate in a free and open government.

> ***Access to such information should not be thwarted by shrouding it with the cloak of secrecy or confidentiality.***
>
> McKinney's Public Officers Law § 84

For the reasons stated below, publicly owned open source optical scanners, combined with sufficient public oversight and scrutiny of the optical scanners, is our second best democratic option to preserve accountability and control over our public business – the government.

> ***The legislature therefore declares that government is the public's business** and that the public, individually and collectively and represented by a free press, should have access to the records of government in accordance with the provisions of this article.*
> McKinney's Public Officers Law § 84 (emphasis supplied)

New York has the burden and the benefit of learning from the experiences of a nation that purchased these shoddy computers, exposing the country to huge security risks as a result of the hidden and not so hidden vulnerabilities of these systems. Indeed at this late date, it would be irresponsible for New York to now blindly follow by purchasing these same machines. At the same time, choosing a publicly owned, open source paper ballot optical scan voting system that integrates public oversight to the greatest extent possible, would show leadership and direction for the rest of the nation.

Democratic Elections: Restoring Transparency and Oversight Using Open Source Paper Ballot Optical Scanners Along With Public Oversight

Unlike the closed proprietary software the major voting vendors choose to use, open source software is open and free under the General Public License (GPL), which allows anyone to use, distribute or alter the software, but not to sell it. It is a relatively revolutionary concept in the world of intellectual property which empowers the collective to contribute and thereby enrich the software development while retaining a public and therefore more highly scrutinized (or 'watched', recall the term 'watchers' historically and continually used in our Election Law) product. This makes for a computerized voting system that while still not failsafe (since no computer can be), is a more reliable system when combined with public access to the optically-scanned paper ballots and a partial hand count to check the computer (see endnote 12).

Open source code optical scanners begin to restore some of that transparency which would be eliminated by private vendors who bar the public from access to any source code information. The advantage of open source software is that it is available for public inspection by anyone with some level of computer literacy, not just those designated to see the escrowed source code pursuant to a non disclosure agreement (NDA). While this is still not the full public scrutiny that manual hand counting would allow, in that the general public still needs to rely on experts to scrutinize the source code, it is clearly more desirable than excluding the public from access to the very information that directs all functions of the voting machines, including vote counting. And it is a step more consistent with the democratic understanding that these are the people's elections and it is the people who must ultimately hold its government accountable; something we can not do if the government and private vendors are the only ones with access to the deemed proprietary information.

Open source software does not need to be archived like proprietary software because it's already publicly available to be examined: a far more desirable solution than what our current source code escrow law provides in New York, under any of the varying interpretations the State Board of Election (SBOE) is debating.

It is to be observed that only a non-privatized, open source, paper ballot optical scanner can be considered as a step towards maintaining control of the public's elections. Open source optical scanners can be audited by permitting the public to examine the ballot images of the physical ballots and checked by a partial hand count to discern the optical scanner's potential for error, malfunction or manipulation. DREs, on the other hand, have no means to verify the outcome of elections.

If we have learned anything over the past six years from the extensive testing and documented failures of DREs it is that there is no way to adequately safeguard this technology. Because there's nothing publicly observable on a DRE the public can never know that their ballots were counted as cast, an integral part of the constitutionally protected franchise. Even with a paper trail (VVPAT), studies show that an adequate proportion of the voters don't check the VVPAT in detail such that discrepancies might be detected [5] and that even if voters were to check the VVPAT, both the paper trail on a DRE and the electronic tally can be rigged such that both would agree and both could be wrong. [6] Indeed it was the Carter Baker Report [7] that observed:

> *DRE software can be modified maliciously before being installed*
> ....
> *If DREs can be manipulated.........the same can be done with paper audit trails*

Accordingly DREs are not a viable voting system with or without open source software, but open source optical scanners can be verified by the people if sufficient public scrutiny is protected by law.

It is not enough just to make the source code publicly available, although that is a first step. We must enable the necessary transparency and accountability, eliminated by the major vendors, by releasing for public inspection the ballot images of our scanned paper ballots. Making the ballot images available to the public on the Internet or CD provides for an immediate, inexpensive and comprehensive audit by the public as well as by election officials[8] and a partial hand count on election night permits citizens the check against the invisibility created by the computer (see endnote 12).

A New York State-Controlled Open Source Optical Scan Voting System Integrating Public Oversight is a Far More Secure System Than Anything Offered by the Conventional Vendors

Foreshadowing our nation's current crisis precipitated by having surrendered control of our elections to private corporations that count our votes in secrecy, the late NYU professor Irwin Mann, wrote in 1993:[9]

> *The advent of computer technology will inevitably affect all the systems that we use for voting and for recording tallies in public elections.* ....
>
> *It is the security of the electoral outcome which may become most at hazard. In the absence of the installation of prudent precautions, the machine and the process shall likely be more vulnerable to large inadvertent errors, and much more ominously, to electoral fraud. The essential reason for this is that, with the technological sophistication,* ***the internal operation of the machine will be less apparent and therefore less apprehensible by the wider public.*** ....
>
> ***It is often proposed that the guardians of software fidelity will be its vendors together with the administrators of the election (public, private, or both). But this degree of trust in such matters surely cannot be,*** *for the future, always warranted.* ***The safeguards must also include the practiced scrutiny of the public. It is fair to say - though perhaps shocking to realize - that a government itself is by far the greatest threat to insufficiently regulated fair elections. ....***
>
> ***For this and similar reasons, there cannot be a relatively small group of persons who exclusively have access to, and control over, the inner workings of an election process****. In order to ensure that such an insulated group cannot occur, we conceive of a condition under which this insulation is virtually impossible. We provide a paradigm whereby the voters have relevant access to the accountability of the voting process. We refer to such a system as an "open voting system".* ....
>
> *In particular,* ***this means that the system can have no proprietary parts!*** ....
>
> ***This open protocol, in conjunction with the standard protocols of a rigorous auditing trail, and sufficient redundancy (including the existence of hard copies of ballots) is essential for full accountability of the system. It will enable the public to serve as watchdog*** *in ways foreseen, and ways perhaps not yet foreseen. The accountability is accomplished by means of the possibility - not necessarily taken up in many cases - of public monitoring of any or all of the components of the system.* ....
>
> ***In the environment of such an open system, any attempt at tampering with an election***

> ***would incur a considerable risk of detection.   ....***
>
> ***Alternatively, if the system is not open, there can never be complete accountability and the public will never have complete confidence in the electoral process. The public itself must be the ultimate watchdog and guarantor of faithful elections****.*
> (emphasis supplied)

In addition to preserving the integrity of the electoral process by insisting on a transparent voting system that the public can monitor, open source software contributes to this goal because the software has been openly scrutinized by the larger audience of software development peers who have had the opportunity for public inspection; a process that cannot occur with secret proprietary software. This allows the best independent technical experts to analyze the source code and publish their findings. As Professor Wagner of UC Berkeley testified before the House of Representatives in March of this year:[10]

> *The value of independent evaluation is probably most pronounced when it comes to security. Security flaws can sometimes be subtle and easy to miss, even for experts. For this reason, enabling more people, especially security experts, to review the software significantly increases the likelihood that security problems in the code will be found.*

Permitting a greater community to identify bugs[11] so they can be corrected *before* they cause problems, provides for a better quality and more secure voting product and is consistent with the path New York has followed in waiting to select the best equipment that complies with higher standards. Of course even a better quality open source optical scanner is still not tamperproof as no such technology exists. That is why public oversight enabled by allowing the public to examine the physical ballots on line or on CD, and by checking the potential for error or manipulation of the optical scanner, with a partial hand count [12] are essential aspects of the overall voting system I am proposing for New York – consistent with HAVA, consistent with New York Laws, consistent with Democracy.

Broader disclosure of voting system source code also facilitates holding test labs accountable. Given the abysmal history of testing labs in the nation, which New York has now experienced first hand, one wonders what these labs are qualified to do given how many machines have been certified with such serious defects and documented failures.[13] An open source system enables independent evaluation which not only provides local election officials, the public, and political parties with such independent opinion, but deters the closed loop / lack of accountability these testing labs have enjoyed to date. The secrecy surrounding proprietary source code has been a hindrance to independent evaluation of machines and contributes to the distrust the nation correctly experiences.[14]

Open Voting Solutions has Developed One Such Open Source Optical Scan Voting System

Open Voting Solutions (OVS) has made available a public solution using open source software utilizing commercial off-the-shelf (COTS) hardware. Thus all the software is available for inspection, including the driver as well as the election management software (EMS). None of the other vendors under consideration in New York can make this offer. In addition to the benefits of an open source voting system described above, OVS has developed specific features to further insure the security of the computerized aspect of the electoral process.

Ballot Imaging

The OVS system preserves essential data by creating an image of the front and back of the scanned paper ballot, recorded and stored on the optical scanner, as well as retaining specific data indicating whether or not the boxes have been filled in or checked. These ballot images can and should be made public immediately after the closing of the polls, thereby deterring fraud while providing the transparency democracy requires. Capturing the image of each ballot a voter casts also helps identify fraud in that a record of exactly what votes were cast before the polls close exists so adding ballots after the polls close is made difficult.

In the event that voter intent must be discerned in the counting or auditing of the ballots, because the ballots are readily viewable on the computer they can be blown up to enable the clearest visual of the marked ballot.

Assisting Auditing/Preventing Fraud

The OVS system provides ballot numbering with random, non-sequential numbers. These numbers mark each ballot, but are not associated in any way with any particular voter. Instead, the numbers are unique to each authorized ballot. This not only makes an audit of ballots feasible by checking that each ballot number is part of the collection of valid numbers enabling the accounting for every ballot in each election batch, but makes it more difficult for ballot stuffing fraud or for ballots to go missing. By submitting ID numbers (not serial numbers) and generating these numbers in a fresh collection for each election, fraudulent copied ballots could be detected by the tabulation program. To assist the scanner in catching fraud the ballot number on the ballot can also be expressed as a bar code to further improve computer security.

Under voting / Over voting

Should the OpScan detect an overvote, the ballot is returned to the voter (as spoiled). The voter is then instructed to take the ballot to a supervisor to have the spoiled ballot destroyed by marking and invalidating it, but the supervisor will also keep that spoiled ballot in a separate locked box so that it's available for auditing purposes. The voter is then given a new ballot to recast. Should the voter undervote, the voter is given a warning in case the voter didn't intend to under vote. This gives the voter the opportunity to indicate the choices on the ballot as intended and then return the ballot to the scanner.

The standard OVS machine can be used for both abled and disabled voters

The advantage of a standard OVS Opscan is that the same machine functions for both abled and disabled voters. An election worker can change a standard machine to a handicapped machine and vice versa. The OVS Opscan includes software to allow voice voting [with an addition of a headset--mic and earphones], substitution of a touchscreen monitor for the standard monitor [permits touching to indicate vote], and physically handicapped access with [sip/puff and other substitutes for the mouse]. There is no added price for the capability except for the devices. Ear phones/mic in the form of a headset costs about $10, a touchscreen substitute monitor costs about $175 extra, and the special access sip/puff devices cost a couple hundred dollars. This flexibility helps make full handicapped support feasible in all polling places, particularly in our smaller polling places which otherwise would have to invest in additional equipment for a small number of disabled voters.

Larger Scanner

New York's full face ballot requirement would be greatly facilitated by a larger scanner which OVS can accommodate. OVS can provide scanners that are either 17 x 24 or 81/2 x 34.

New York State's Creating its Own Ballots

Creating ballots for each election is made difficult such that counties often contract this work out to the vendors, a time consuming and expensive aspect of the election every year. OVS has simplified the system so that anyone who can word process can create the ballots. The procedure OVS has created enables public employees to create the ballots for each election in a couple of hours, as opposed to the weeks required when this work has to be sent out to the vendor. Because OVS trains county election employees to do this, the cost savings is also significant and the State retains control over the creation of its ballots.

Over all Cost Savings

The advantage of using off the shelf hardware as compared to specialized voter hardware is the most significant cost savings compared to purchasing these machines from the major vendors. In addition because the software is free and public, there are no annual recurring payments to vendors for use of equipment or software already delivered (the recurring payments private vendors collect for use of their equipment can in some cases double the purchase cost of equipment within a few years of purchase). In addition the benefit of being able to utilize state employees to run and maintain these optical scanners has value in excess of the cost savings, as described below.

Avoiding the Captive Customer Business Model of the Major Vendors which Increases Costs and Undermines the State's Ability to Control its Own Elections

OVS' s business model – in distinct contrast to the conventional vendors who, judging by the experience of the rest of the nation, encourage dependence on them to run their systems and hence our elections – integrates and relies on the training of NYS public employees to run and service the voting equipment. Freeing New York from the captivity of vendors is critically important if New York is to retain control of decisions regarding the way elections should be run.

At the present time the SBOE is only considering the machines and business model of the conventional vendors, placing New York in a position of dependence that undermines the State's ability to direct and control elections as necessary. "The business model of the major vendors is based on locking in counties as a captive customer of a single vendor.... Vendors use the proprietary nature of their code as one tool to keep counties captive".[15] Such exclusive dependence on the vendor is far more costly to New York, not only in terms of money, but in loss of control.[16]

It is important for New York's purposes to note that because a system like OVS's is intended to be specifically customized for the needs and laws of a particular state or precinct, the OVS features described above – which were designed with the intention of integrating transparent and redundant auditing features to enable fuller and more transparent checks and balances of the computerized system – can be readily accommodated to comport with New York's requirements and higher standards in a way conventional vendors are unable and unwilling to do. The flexibility to make these accommodations quickly and easily are a distinguishing factor giving New York the control over our elections not possible when private corporations must be appealed to for changes to the equipment they produce on a mass scale for many states[17]. This, combined with OVS's integration of our public employees as part of its voting system, provides New York State with the freedom it needs to create an electoral process in accordance with the demands of a constitutional republic.

New York Needs to Rely on Our Public Employees, Not Private Vendors, to Conduct Our Elections

Having to depend on private vendors to run our elections, most of whom have openly demonstrated partisan leanings and assert the right to confidential proprietary information about how their machines are programmed to process and count our votes, is a threat to the stability of a democratic society. Private vendors are not accountable to the people nor to the constraints and ideals of a democratic society.

Our public employees, on the other hand, are accountable to us in a way that private vendors are not. The Public Employees Federation (PEF) issued a unanimous resolution in 2005 in which they opposed the privatization of our elections, proposed a ban on contracting with private vendors, and supported paper ballot precinct based optical scanners to be operated and maintained by public employees. [18] As the resolution recites out public employees "are automatically bound by the Public Officers Law which assures transparency, and accountability to the public, and contains prohibitions against partisan political activities."

Indeed I would submit that permitting these vendors, who exert the degree of control over our elections both by their captive business model and insistence on secrecy, to have anything to do with our elections, is violative of the Public Officers Law which requires the avoidance of "conflict between private interests and official duties".[19] We have seen a rededication to these ethical principles intended to protect government transparency and accountability under Governor Spitzer who understands:

> *A continuing problem of a free government is the maintenance among its public servants of moral and ethical standards which are worthy and warrant the confidence of the people.* ***The people are entitled to expect from their public servants a set of standards above the morals of the market place****. A public official of a free government is entrusted with the welfare, prosperity, security and safety of the people he serves.* ***In return for this trust, the people are entitled to know that no substantial conflict between private***

> ***interests and official duties exists in those who serve them.***" (emphasis supplied, see endnote 19)

It is irrational to impose the highest ethical standards on our public servants only to have unaccountable private interests dictate the means by which we elect those public servants. It is equally irrational to permit private interests – who would deny the public access to the very information as to how our elections are processed and counted – to be part of our democratic elections.

We are already witnessing the unacceptable consequence of inviting private interests into our democratic electoral process. In the closing week of the last legislative session Microsoft, who had been attempting to have the SBOE bend the rules to accommodate Microsoft's interest (all of the vendors, OVS being the only exception, chose to use Microsoft's products as part of their closed voting system) attempted to have legislation passed for its and the vendors' benefit. [20] The legislation would have permitted source coding from being escrowed and allowed the vendors even greater secrecy than they currently enjoy under NY's law.

As set forth in greater detail at endnote 20, under our current law the vendors are required to escrow source coding so that a few select people in the government, pursuant to a non disclosure agreement, can view the codes. While our current law goes further than many other states in imposing this escrow requirement, it still defers to the confidentiality demanded by private interests in that the government officials who are permitted to view the escrowed source code are enjoined from sharing that information with the public! Barring the public access to information about their elections, which rightfully belongs to them, is antithetical to the notion of free, fair and open elections.

This is precisely why New York cannot permit the privatization of its elections and be forced to capitulate to the claimed proprietary rights of voting vendors or Microsoft. If there is one public domain that must resist private interest prerogatives, it is the people's elections.

Conclusion

New York State government has a responsibility to its citizens to support the Constitution and to faithfully discharge the duties imposed by the Constitution. Accordingly, as I concluded in my Memo I, *The voting vendors scheduled for certification testing are ineligible to contract with New York State,* New York cannot compromise its citizens' constitutional rights by delegating control of this fundamental responsibility to private corporations, particularly when they are claiming entitlement to conceal vital and public information from the citizens of New York State.

New York must provide a voting system which "...secur[es] *to all citizens...the right freely to cast their ballots for offices to be filled by election and* ***the right to have those ballots****....* ***received and fairly counted****.*"[21]

> *The right of the elector to vote is conferred by the Constitution, and he ......* ***is entitled to see that his vote has been given full force and effect*** *in the determination of what persons have been elected to office.*[22]
>
> *Deister v Wintermute,* 194 NY 99, 109 (Court of Appeals 1909)

The systems offered by the major vendors deprive the public of transparency and hence the ability to monitor/oversee their elections. Only a publicly owned and controlled electoral process can be considered constitutionally acceptable.

ENDNOTES

1. See my Memo I*, The voting vendors scheduled for certification testing are ineligible to contract with New York State*

2.See the report of the federal government's technical advisors, the National Institute of Standards and Technology (**NIST),** http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf, **which found DREs** ***"are vulnerable to errors and fraud and cannot be made secure." "The DRE provides no independent capability to detect whether fraud has not caused errors in the records...... a single... programmer ...could rig an entire statewide election".***
The NIST research staff further stated that they "*do not know how to write testable requirements to satisfy that the software in a DRE is correct".*

The report of California's Voting System Technical Assessment and Advisory Board (VSTAAB) http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf, (confirming the findings of the Hursti Hack, Black Box Report Security Alert: July 4, 2005 Critical Security Issues with Diebold Optical Scan Design (1.94w), 2005, http://www.blackboxvoting.org/BBVtsxstudy.pdf) which found that Optical Scanners can be hacked without detection. The California report, commissioned by California's Secretary of State, warns: ***"successful attacks can only be detected by examining the paper ballots. 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.*"**

See also the Government Accountability Office's (GAO) reports, which have on two occasions expressed **concerns that the problems with electronic voting systems are so pervasively problematic they "could damage the integrity** of ballots, votes and voting-system software by allowing unauthorized modifications." October 2005 Report http://www.gao.gov/new.items/d05956.pdf And see the latest study, released March 7, 2007, http://www.gao.gov/new.items/d07576t.pdf,wherein the GAO Information Technology Architecture and Systems Director, Randolph C. Hite, testified that electronic voting systems can break an election!

"***[E]lectronic voting systems are an undeniably critical link in the overall election chain. While this link alone cannot make an election, it can break one****. The problems that some jurisdictions have experienced and the serious concerns that have surfaced highlight the potential for continuing difficulties in upcoming national elections if these challenges are not effectively addressed"*

See also Bruce O'Dell's, *Open Source Voting Considered Harmful*, http://www.opednews.com/articles/opedne_bruce_o__061027__22open_source_voting_.htm

"The level of protection required to secure voting software far surpasses financial software, but it also certainly deserves far greater protection than mere safety-critical software. Planes can crash, chemical plants accidentally vent noxious gases, and medical devices can malfunction - while our democratic way of life goes on, for everyone but the unfortunate few. ***Voting systems are national security systems. Compromise voting systems and the outcome is as disastrous as invasion and occupation by a foreign power – even worse****. Conquest by exploitation of voting system vulnerabilities not only preserves a country's economy in whole to facilitate plundering, it appears to occur under the guise of the free exercise of the democratic franchise, manufacturing the fraudulent appearance of the consent of the governed while pre-empting resistance."*

3. See recent account of protocols for hand counting at http://www.smirkingchimp.com/thread/8842

4. See NIST report referred to at endnote 2.

5. A 2005 study by the Caltech-MIT Voting Project, http://www.vote.caltech.edu/media/documents/wps/vtp_wp28.pdf , "concluded the following:

> *no errors were reported in our post-survey data ... ... and over 60 percent of participants indicated that they were not sure if the paper trail contained errors.*

That's right: in test elections full of deliberately engineered VVPAT errors - including swapped votes and even missing races - no one reported a VVPAT error while voting, a majority were unsure whether there were any errors or not, and almost a third of the participants continued to insist that there no errors at all even after they were told otherwise by those who switched the votes.", from Pull the Plug on E-Voting & Pull the Plug on E-Voting, Part 2

And as a recent paper, http://chil.rice.edu/research/pdf/EverettDissertation.pdf, reveals:

> *[A]s the situation currently stands, voters cannot be depended upon to check the validity of their vote. Many security experts and election reform groups are calling for VVPATs to be required on*

> *all DREs and as of the 2006 elections, nearly half of the states mandated that their DREs have paper trails (electionline.org, 2006). However, these studies show that solutions to DRE security problems that require voter verification of their ballots may not solve vote-flipping problems. Users are not even checking their ballots on the review screen that is presented directly in front of them.*
>
> *The findings here suggest that it is highly unlikely that voters will detect changes to their ballots on the VVPAT that prints out on a roll of paper next to the machine if they are not even noticing them on a screen presented directly in front of them.*

6. Technology Review: How to Hack an Election in One Minute: Princeton U. researchers have released a study and video that demonstrate the ease of altering votes on an electronic voting machine, http://www.technologyreview.com/Infotech/17508/?a=f And see the study at http://itpolicy.princeton.edu/voting/ts-paper.pdf

7.Carter Baker Report, http://www.american.edu/ia/cfer/

8. Professor David Wagner of the University of California, Berkeley, testifying before the House of Representatives in May, 2007, http://www.cs.berkeley.edu/~daw/papers/testimony-oversight07.pdf , describing what could be done to start restoring the transparency lost to the rest of the nation as a result of the privatization of elections:

> *The single most important step that local election officials could take to improve transparency would be to institute routine manual audits and allow public observation of these audits....Audits provide a way to assess the accuracy of voting software. They are one of the few opportunities for a voter to verify that the votes were counted and tabulated correctly by the voting equipment. Election officials should ensure that interested parties are able to observe all aspects of the audit and see for themselves that the votes were counted accurately.*

9. http://www.cpsr.org/prevsite/conferences/cfp93/mann.html

10. Testimony of Professor David Wagner testifying before the House of Representatives in March, 2007, http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf

11. See Bruce O'Dell's, *Open Source Voting Considered Harmful*, http://www.opednews.com/articles/opedne_bruce_o__061027__22open_source_voting_.htm

"Open source" software is just one small component in the end to end voting system, which includes not just tabulation software, but a vast array of other computer components such as operating systems, firmware, and device drivers. Consider that even if Diebold's optical scan software operated with perfect fidelity it could be subverted through careful exploitation of integer overflow vulnerabilities using its peripheral memory card in such a way that the hypothetical pure-as-the-driven-snow software would be unable to detect that a bias had been introduced. And consider the process of deploying that vast array of components with total precision on hundreds of thousands of target devices in the field; that's hardly "open source". That's all done by people.

So more fundamentally: I consider all the output of a computer at all times to be suspect unless and until it is verified. Some of my colleagues feel the reverse; that we should trust the output of a *computer unless we can show how it could be compromised. That shows a charming faith in other people's fundamental good nature, but that's no way to run a bank - or an election.* ***When it comes to the integrity of computer systems that can quite literally take away my liberty, I don't accept "trust me*** *- you don't need to double check this", and neither should you.*

As a consequence*, Jonathan Simon and* ***I have shown that to even consider using optical scan devices, you need a secure hand count audit of a least 10% of the ballots in a congressional election****. And potentially more to protect elections with fewer than 150,000 voters.* ***You need to perform this audit*** *whether it's Diebold's Jeffrey Dean, or Avi Rubin, or Alan Turing himself come down from Heaven, who writes the tabulation code.* ***Because you simply don't, can't and never will be able to know - with sufficient certainty to possibly throw away the American Republic - what each of those thousands of optical scan devices are actually doing unless you check their output. By hand.*** ....

Voting systems are national security systems. Compromise voting systems and the outcome is as disastrous as invasion and occupation by a foreign power – even worse.

See David Wagner's Testimony before the US House of Representatives in March, 2007, http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf

Source code disclosure alone cannot ensure that voting machines are trustworthy, because even the most open source code analysis cannot guarantee that a voting machine is secure, reliable, accurate, fair or fit for use in elections. This is due to two reasons. First, it is often difficult to be certain that the source code one is analyzing is the same as what will be executed by the voting machine on election day. Second, given the complexity of election-related software, it is generally not possible to be certain that you have found all the bugs in the software, and it is generally not possible to be certain that the software will work reliably and accurately on election day. This means that source code analysis can be used to show the presence of defects in voting software, but usually it cannot convincingly demonstrate the absence of defects. Source code analysis alone is unlikely to be able to demonstrate that voting machines are trustworthy.

See Joseph Hall's *Transparency and Access to Source Code in Electronic Voting*, http://www.usenix.com/events/evt06/tech/full_papers/hall/hall.pdf

Of course, bug finding is just one example of security-increasing research applications that source code availability could catalyze.

From a systems perspective, evaluation of code is not enough. Even in analyses outside of the ITA process, critical flaws have been found that only become evident when testing the integrated system. We must also include other techniques such as adversarial testing, parallel monitoring, reliability testing and forms of feedback that we have in other areas of computing such as incident reporting and feedback.

Of course, source code availability does not address comprehension; most voters will not gain any more insight into the operation of a voting system when source code has been made available to them. However, the mere fact that it is available and that they or a trusted representative could examine it will increase the level to which they trust these systems.

Acknowledging that this form of limited source code disclosure does not support general public scrutiny of source code, and therefore does not fully promote the transparency goals that we have articulated, we note that in a public source code disclosure or open source code model most members of the public will be unable to engage in independent analysis of the source code and will need to rely on independent, hopefully trusted and trustworthy, experts.

12. *Landslide Denied,*
http://www.electiondefensealliance.org/landslide_denied_exit_polls_vs_vote_count_2006

> The report describes the specific means of effectively conducting a public hand count of 10% of the paper ballot records in 100% of the precincts in federal and statewide races. The UPS is to be conducted "in-precinct" on election night, by citizens representing all concerned political parties, and open to general public observation. Because it is conducted in-precinct, the UPS avoids the difficult task of protecting the chain of custody of paper ballot records in 180,000 U.S. precincts. In fact, all the alternative after-the-fact "spot-audit" schemes impose this monumental burden – since in all those protocols, all precincts must safeguard ballot records until just a few percent are "randomly chosen" some time after the election. Integrity of the chain of custody will be especially suspect, of course, in just those suspect elections which such audits are proposed to safeguard. Since a 10% hand-count sample would be drawn in 100% of precincts on election night, the UPS also eases the transition to decentralized, citizen-monitored hand-count verifications of elections, placing responsibility for the integrity of the vote count in the hands of the American people, where it rightfully belongs. Most importantly, the UPS is inherently resistant to manipulation. The report describes how any attempt to systematically manipulate the UPS audit would be extraordinarily difficult to conduct and to conceal. Not only would it require a very large number of participants, any effort to skew the 10% paper hand count in favor of a candidate would be very likely to increase the overall discrepancy, not decrease it.
>
> In order to restore and maintain citizen trust in the integrity of American democracy, it is critical that wherever electronic vote tallying is performed, paper ballot records must always be produced and must always be checked by the best possible "security mechanism" – the American people, working together in public.

13. See, The Dirty Little Secrets of Voting System Testing Labs,
http://www.huffingtonpost.com/avi-rubin/the-dirty-little-secrets-_b_12354.html_

14.March, 2007 testimony of Wagner before the House of Representatives
http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf

There are several steps that could be taken to restore some of the transparency that has been lost:

> Reversing the presumption of secrecy for technical information about voting technology would make it possible to have a more informed debate on the trustworthiness machines. In particular, disclosure of source code would allow interested parties to analyze the software for themselves, without having to rely upon analysis from some testing lab. We could expect and insist that anyone who wants to argue that the voting software from one vendor is flawed should be able to point to where exactly in the source code the flaw may be found. We could expect and insist that anyone who wants to argue that the voting software is flawless should be able to show evidence that the source code is free of flaws. This would create the opportunity for a more informed and scientific debate regarding the trustworthiness of e-voting, and it might raise the level of the debate.

15. March, 2007 testimony of Wagner before the House of Representatives
http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf

16. In addition to the total dependence created by the major vendor business model, the vendors have also exercised the kind of control over the national election process that only companies with some monopoly control and a wink from the federal government can exert. We have seen how their money buys influence over testing, over contracts, over election and election officials, over legislation. This is extremely unhealthy for a democracy. See for just one eg. *Corporate Control of the Election Process* by John Gideon and www.votersUnite.org, http://votetrustusa.org/index.php?option=com_content&task=view&id=86&Itemid=845

17. This is in marked contrast to the approach of conventional vendors who have used the courts and the state legislators to try and override state's laws and rules written for the benefit of their citizens. Because the vendors choose to use proprietary software and because they profit by making products that can be sold in all states, those states with higher standards, like New York, find themselves battling with vendors who would rather see the state bend to the vendor's lower standards and the limitations of the products they have to offer. See my Memo I, *The voting vendors scheduled for certification testing are ineligible to contract with New York State* at pp 35-39 and at p 21:

> *The example of Diebold, in choosing to ignore North Carolina's law and then seeking to evade it at the 11th hour, is precisely what Avante and Microsoft are doing in New York at the present time. All of the major vendors chose to use Microsoft's products, thereby voluntarily making themselves unable to comply with New York's 2005 escrow requirements. (see discussion of this issue at pp 35-39)*
>
> *Avante's and Microsoft's tactics show insulting disregard for the laws of a sovereign state and a brazen willingness to disrespect those laws with the intention of later strong arming the powers that be in order to override the law. It is a direct consequence of the privatization of our elections, particularly when those private corporations have a monopolistic hold. As discussed at the Conclusion, this is one of the compelling reasons why New York must resist falling prey to such domination if it is to abide by our Constitution and the rights of its citizens.*

18. http://nyvv.org/doc/PEF_opscan_res1.pdf . It should be noted that a publicly available open source optical scanner was not available in 2005 when this resolution opposing privatization and DREs was approved.

19. Quoting from the Historical and Statutory Notes of the Code of Ethics contained in the Public Officers Law, Declaration of Intent, McKinney's Public Officers Law, Section 74.

20. See Bo Liparis web log at New Yorkers for Verified Voting http://nyvv.org/blog/2007/04/microsoft-says-we-wont-escrow.html, ***Microsoft Says We Won't Escrow: Software Giant Tells New York "Forget about it"***:

> *On Friday, April 13, 2007, the New York State Board of Elections notified vendors hoping to certify voting systems in the state that Microsoft would not comply with the source code escrow requirements of state election law.* ....
>
> *With Microsoft unwilling to place source code in escrow, voting systems which use Microsoft products are not eligible for certification and use in the state.*
>
> *New York State Election Law, Section 7-208 states that the voting system vendors "shall place*

> *into escrow with the state board of elections a complete copy of all programming, source coding and software employed by the voting machine, system or equipment.* ....
>
> *The State Board had been holding discussions with Microsoft in order to determine how compliance with State Election Law would be met. The Board also submitted a list of questions to Microsoft about the escrow issue. In these discussions and answers, the software giant indicated that it does not and will not put its source code in escrow accounts, and it does not and will not escrow source code through any third parties or the National Institute of Standards and Technology. In other words, the Redmond behemoth is telling New York State, and any other states that have a high legal bar for escrow and review of software source code, "Forget about it." Microsoft, which has only recently begun to weigh in on voting system software proprietary claims, is taking the same stance that voting machine vendors have always taken – the public cannot have access to the software we vote on.*
>
> *One of the questions the* ***State Board of Elections asked Microsoft*** *was: "****If there are significant problems with the law as written and those problems would preclude us from agreeing to an escrow arrangement, are there any changes to the law that Microsoft would suggest?" Ah yes, let's be sure to let the private corporations of the world have their say in how our election laws can be changed to better serve their interests.*** *Stay tuned.*

In June Microsoft rewrote our legislation and tried to have it passed in the final chaos of the legislative session. See ***Microsoft Muscles the NYS Legislature*** http://nyvv.org/blog/2007/06/microsoft-muscles-nys-legislature_16.html

> **Software giant moves to weaken NY Election law**
>
> *The 800 pound gorilla of software development has moved forcefully into New York State, supported by voting machine vendors using Microsoft Windows in their touch screen voting machines and other systems.* ***Over the last two months Microsoft and a cadre of high paid lobbyists have been working a full-court press in Albany in an attempt to bring about a serious weakening of New York State election law.*** ....
>
> *On Thursday, June 14, I received a copy of proposed changes to New York State Election Law drafted by Microsoft attorneys that has been circulating among the Legislature. These changes would gut the source code escrow and review provisions provided in our current law, which were fought for and won by election integrity activists around the state and adopted by the Legislature in June 2005.* ....

21. Quoting from *Hopper v Britt*, supra at 151, which language was taken from the Court's ruling in *Goring v Wappinger* Falls, 144 NY 616, 620-621, both Court of Appeals rulings.