

Ted Selker, PhD Computer Science  
Jon Goler  
Caltech/MIT Voting Technology Project  
April 2004

**Attack name:**  
**Security Vulnerabilities and Problems with VVPT**

Applicability

This is a method of defrauding a paper trail record

Attack method

Designers use statistical assurances that voters don't verify paper trails as a premise. They design the paper trail software to misprint a few enough paper trails that it will go unnoticed but disrupt the election results.

Resource Requirements and cost

The cost is the same as any other electronic fraud in electronic voting system cost

Consequences and potential gain

The opportunity to defraud election results

Likelihood of detection

Must be verified by a camera or other enough parallel testing.

Countermeasures

Video verification of paper verification. Parallel testing, Nversion system,

Retrospective and historical notes

This approach came to us after watching how difficult it is for people to verify paper trails

**Abstract**

A proposed Voter Verifiable Paper Trail (VVPT) includes a printed ballot as a receipt that a voter can view to verify their vote before leaving an electronic voting machine. This method is also supposed to insure the accuracy of the recorded vote by allowing the tally to be checked later by counting the collected receipts.

This paper considers problems with ergonomics, logistics, security, fraud, and mechanical fragility with using VVPT. Ergonomic problems are introduced by the receipt having a different layout than the ballot, difficulty remembering previous selections to make the verification, by the extra step it introduces after making selections and by it not working well for sightless people. Logistics problems include difficulties in collecting and organizing the receipts, transporting them, and reading and reconciling them with electronic tallies. Security issues include the possibility that receipts can be systematically misprinted in a way that cannot be detected and that hand counting will not easily detect fraud. Mechanical problems include printer breakdowns and supplies running out. VVPTs could add problems by being questioned in various ways or though the development of computer programs that defraud the VVPT systematically. VVPTs do not address existing sources of disenfranchisement such as registration problems, equipment and ballot problems, and polling place problems.

Experiments and elections have yet to establish that people can in fact verify their ballots using a paper receipt. Effective approaches for accurately counting the paper receipts for auditing purposes have not been established either.

Proving that an election correctly records and transmits the intention of the voter is worthwhile. Computers are the first technology that can easily report voting results in multiple formats. Simple systems-verification solutions are possible. Parallel voting and time shifted testing require no extra equipment. Voter Verified

Audio Transcripts would simplify voting and improve audit security by presenting verification as feedback during the selection process rather than post hoc auditing. .

## Introduction

Choosing a government is contentious and the mechanisms for collecting and counting votes have always been on the minds of the people involved. In ancient Greece, Egypt, and Rome people used physical objects, like shards of pottery, to document their choices. Over the last century, developing voting technology has continued to improve the way votes are marked and collected. In 1868 Thomas Edison invented an electronic voting machine. In the 1890s the so-called "Australian secret ballot" was adopted in United States. Hand transcription of marks on paper has given way to automated optical sensors reading the marks. Automated counting reduces the problems of people overlooking, adding, or removing a mark. Writing down columns of local tallies to be added together by hand has given way to spreadsheets and automated calculations. These methods further eliminate human errors. New computer voting machines will not let voters make the mistake of leaving extra marks on alternative selections or making too many selections for a race. Automated processes are eliminating some errors, as well. Prospects are good for using technology to simplify the voting user experience and increasing its accuracy.

However, all technological improvements raise questions and must be implemented in a controlled way. In the case of voting technology, improvements have required experiments, slow rollouts and adjustments. Brazil introduced electronic voting in stages. In 1996, Brazil put electronic voting into place for 40,000 voters with 7% not being able to succeed at recording their votes electronically. Improvements from that experiment allowed this rate to fall to 2% for the 150,000-person experiment 1998. Improvements from that experiment resulted in only an estimated .2% of 106 million voters who were unable to electronically deposit in Brazil in 2000.

User experience problems plagued the early electronic voting machines introduced in this country; in some cases the number of votes that were left unmarked on the new machines was greater than for the equipment they replaced. For example, some electronic ballots placed the selection to scroll to the next race too close to the selection for depositing the ballot, causing some voters to inadvertently cast their ballots before completing it.

In accordance with law, the paper punch cards from the 2000 Florida election have been destroyed. Many people believe that we will never know the intentions of the voters in United States 2000 presidential election. Forensics [1] shows that 2 to 3 percent of the votes were lost due to problems with registration, ballot design and polling place operations. These problems are not new or unusual but are dramatized by the closeness of the 2000 presidential race, coupled with the desire to properly vet its outcome in an information-sophisticated world. These simple-to-solve problems are not being addressed systematically. Instead, the public conversation has shifted to more vague issues of technology in elections and fraud.

The call has gone out for approaches that will produce accurate, secure recording of votes with complete integrity [6]. Unlike paper ballots, voting machines give feedback to voters as they vote. Voting machines that disallow voting for too many candidates have reduced disenfranchisement of voters [7]. The common belief is that electronic voting machines will simplify the vote collection and counting process for all. Historically, the fragmented voting industry consisted of several companies that compete for the occasional upgrade. In the wake of the 2000 election, the Help America Vote Legislative Act of 2002 changed this in that it made available \$1.2 billion in 2003 to upgrade the country's voting machines quickly [3]. Are these monies being released to buy machines when it could be better spent researching how to improve them and the processes in which they are used?

Concerns about security of the collection and counting process have always been important. Computers offer the first technology that can easily make copies of information in different forms for archival preservation. Electronic voting machines of today keep records of the votes on disk, removable physical media in memories and, as a final count, on a paper scroll. These multiple records can improve voting machines' immunity to problems. For example, if a floppy disk from the Brazilian Procom voting machine

is unreadable, the election administrator records another one from the internal flash memory in the voting machine.

However, the big question is how can we prove that the selections made on a computer interface by a voter are reflected correctly in the digital voting machine records? Critics of using computers to perform secure operations are speaking up. Broad media coverage has been given to the issue of how we can know that a vote is collected without the computer program tampering with it.

Many approaches to ensure the secure transfer of a voter's selections into the computer are possible [2]. Adequate and provable electronic security could make certain that the vote tallies reflect the voter's intention. A separate Votometer machine can check the voting machine while it is running. Modular architectures can segment the process so that any changes in the votes would take multiple changes to code written by different organizations. Some call for the code being open for anyone to view in a so-called *open source* way. Many believe that separate records that are human readable will be most helpful. Open viewability of a second ballot has seemed attractive to many.

The most popular of these in the public's eye have included Voter Verified Paper Trails (VVPT). The various schemes for this all include a display on which a voter makes selections and a way of viewing a paper receipt that is printed to reflect these selections. The voter cannot take this voting receipt away with them because if they did, it could be used to show how they voted and would compromise the secret ballot and security of elections. Nonetheless, such approaches have captured media and governmental attention as a solution. This paper describes some of the difficulties with VVPTs. A forthcoming paper will describe several alternative verifiable approaches to security.

### **Ergonomics issues**

The VVPT is in a different format than the ballot, in a different place, is verified at a different time, and has a different graphical layout with different contrast and lighting parameters. Handling VVPTs causes other ergonomic problems for the ballot workers. During the first use of VVPT in an election, in November 2003 in Wilton, CT, virtually all voters had to be prompted to find and verify their receipt. This turned into extra effort for poll workers and extra time for voting. Anything that takes a voters attention away from the act of casting a ballot or causes a voter to invalidate their vote will reduce the chances of them voting for the candidate they intended. Many voters are frightened of going to balloting places because they fear intimidations that actually can transpire. They fear the voting process, the technology, and their registration not being there. The complexity of the voting process is already a deterrent from voting; VVPT adds complexity, which could drive away more voters.

People are extremely good at remembering hundreds of precise images and comparing them against the same image [7]. But the format of the paper receipt will be different than that of the voting machine and because of these differences it is difficult for people to compare them after the fact. Most people have had the experience of taking two columns of numbers and finding it difficult to verify that they have not missed a number. Comparing dozens of selections on a voter-verified paper receipt will take such special care. Complications of comparing a separate paper trail in a different ballot format might add extra difficulty for people with learning and reading disabilities. The Wilton, CT experiment found people not noticing the VVPT because it was in a different place in the booth.

Time limits on voting (3 minutes in New York City) are designed to keep balloting running smoothly. This time will likely need to be extended to allow for checking of the voter-verified paper trail. When people are focusing on a ballot it will be extra work to remember that they have to look at another place to verify their ballot.

When a voter deposits his or her punch card ballot into the ESS PBC 2100, an electronic display shows that the voter has not voted for every race correctly, a paper trail is printed showing exactly the races in which a voter did not vote correctly. This system only shows problems that should be attended to and should be much easier to understand than a paper trail. In watching 500 voters casting ballots, I saw less than one in

10 people who, when they were told they had a problem with their ballot, were actually willing to take a new ballot and vote again. There appeared to be four reasons for this: many said they “knew” they had done the right thing and it must be all right, many felt pressed for time and wanted to leave, some were embarrassed, and some seemed overwhelmed. The task of reviewing the ballot after a person believes they have completed the task can be anticlimactic. One thinks they are done with voting but must go through it again.

The biggest difficulty in verifying a paper trail might be that some jurisdictions have over 100 races on which a voter makes selections. Remembering how one voted on each is difficult. Without a reference guide, it is likely that people who make decisions while marking their vote will forget how they marked the ballot that they are checking. Incorrectly calling fraud on a ballot machine will slow or stop others from getting to vote. In any case the difficulty of the cognitive task of checking a ballot afterwards will be much higher than any perceptual task that is required of the voter while they are marking their ballots [4].

The most popular description of VVPT places it behind glass to avoid losing the integrity of the secondary ballots. To the extent that the paper trail is not directly against the glass or the glass is not thick, offset parallax can make it hard to view. The apparent position of a finger against the glass changes with the viewing angle, making it difficult to accurately see which selection is being verified on a ballot with dozens of races.

Additional ergonomic considerations include lighting and readability issues that probably can be dealt with. For some vision-impaired people magnifying glasses and lighting will not make this process more accessible. A different verification mechanism such as audio verification will be required for them not to be disenfranchised.

The step of reviewing the voting machine after using it has been difficult for voters. In Cook County, IL there are videotapes or machines to train people in using the ESS PBC2100. But, in visiting some 60 precincts, I never saw anyone watch the video. Maybe people believe that they can figure it out once they are in the voting machine.

Ballot worker ergonomic problems exist in the logistics of keeping the receipts secure, counting them, verifying that they are the same number as the number in the DRE, sealing the receipts in a transport box, checking that these are prepared correctly for transport (hopefully under scrutiny of more than one person), and transferring them. Ergonomic problems complicating the process turn into logistical problems.

### **Logistics problems**

Collecting and counting the ballots can be difficult. In Wilton, CT the ballot boxes had a gap through which ballots could have fallen. While watching a precinct close down in Cook County, IL in March 2002, we noticed a ballot on the floor. Transporting ballots has posed problems. Even in LA County, in the last use of punch cards in October 2003, a ballot box was lost for several hours. At 2:00 a.m. somebody had to go look for the hopefully-untampered-with missing box; finally it was found behind a door in the polling place. Ballots have been known to fall off the top of cars and have been left in trunks of cars during transportation. There were allegations in the 2000 election of replacing one set of punch cards in a balloting place with another. Typically a ballot worker transports ballots in a personal car to a collection station. In the fall of 2003 San Francisco election, some ballot workers transported paper ballots in shopping carts down the street. These methods of transportation raise serious concerns on the security of votes.

By the time election workers shut down a polling place, many of them have worked a 13-hour day. In LA County we recently saw a poll worker bully others into saying that they had completed checks that only one person actually did. We saw people closing a ballot box and covering the bar code “for security” which would make it unreadable by the machine as it traveled to the paper ballot collection center. These kinds of mistakes with physical things are always an issue for any system that a person is not familiar with or does not do on a regular basis. When people are doing something that is very important, nervousness as well as fatigue can make them less reliable.

Arranging to store and read the ballots later presents formidable problems. Punch card holes are designed to be the simplest of all possible separate paper records to read in an automated way. While it is easy to read one or ten cards, no one has made a reader that can read a million reliably. Being human readable will make it harder to accurately read the ballots with machines. Even when multiple people read ballots together the tally can change with multiple readings. How many hand counts are required to certify correctness? When the number is different between the paper and the electronic, which one should be trusted? Reading scraps of paper or receipts automatically has not been established as reliable. Machine reading Optical Character Reader (OCR) scan ballots, and punch cards, are more reliable than people reading paper [1]. The suggestion that some human -unreadable indicator, such as a barcode, be included on each receipt compromises the VVPT proponent's goal of the humans as the final judge.

The fact that the VVPT is not the primary election count will be known by the ballot workers likely leading them to be less careful with them than with primary ballots. Since receipts are curled thin paper, the process of counting them at the end of the day is harder than counting paper ballots. Not counting them at poll closing will make it harder to validate later.

Receipts printed with paper tape are hard to stack or organize. In Broward County, FL, for example, the ballots are counted in a warehouse where a loading dock door is commonly left open, letting wind blow in that could shift the paper. VVPTs will require workers to handle scraps of paper curled by the roll in the machine. The mechanical problems of handling the thin paper will be worse than with customary ballots. Interpreting the human readable words on them will be more complex than registering a hole or a filled-in oval.

All election machines today allow an administrator to change the time. Changing the time on the voting machine, ballot, or OCR could allow someone to maliciously revote a precinct. Knowing how many people voted for the day, a dishonest poll worker could fraudulently revote the election. The worker could produce a new fraudulent VVPT, putting into question which VVPT is correct. Luckily this would be a labor-intensive way to defraud an election.

Counting the paper trail presents other problems. Ballot workers arranging and moving cards around always seems precarious. Ballot workers who are running a punch card machine have procedures for dealing with misread cards. Even when everyone is watching in an organized punch card reading operation, people worry about cards getting disorganized, out of order, and being removed or changed.

People are inured to paperwork. People who work with computers constantly have to approve long contracts in order to install software. Computer users are used to approving contracts without reading them completely; most just press the approve button. Conversely, for the non-computer users, the very idea of checking a computer might be confusing; how would they know what to trust? Now consider people who go through checkout lines in the grocery store. When I was a teenager I bought food for my family and had to be frugal. The cashier hand transcribed the prices into the cash register; I would check my receipt and often find an error; when in my favor, I was refunded. Today cash registers that scan prices have reduced the problems of transcription of the prices and are more reliable. It is not so common to find errors any more and many people do not look at them. ATMs also give receipts. These receipts often have the balance of a bank account and can even indicate the account on them. Even with important financial information on them, these receipts are dropped on the floor or put in the trash can right next to the ATM where anyone could see them. Being surrounded by receipts that we do not pay attention to is an impediment on taking the voter verifiable paper trail seriously. It is unclear that voters will be more careful with a VVPT than they are in caring for their receipts at an ATM or in a grocery store.

Illiteracy can also be a problem when trying to verify a ballot. Variation in formats between the ballot and a verifiable paper receipt can confuse the voter. Voter information often helps people to familiarize themselves with the ballot they will see on the voting machine or to create a crib sheet to allow them to recognize where to mark the ballot. Unfortunately, the paper receipt is in a different format and would require a separate verification sheet to be tested by an illiterate person.

Less than fifty percent of eligible voters in this country vote. The increased logistical problems introduced by VVPT will not make people think voting is easier.

### **Software Security and Fraud in Voter Verification systems**

A natural question about voting concerns possible fraud. David Orr, the county clerk of Cook County, Illinois, said he believes that only 1/3 of voters who are told they have an overvote will take a new ballot. Others have described seeing only one in 10 to one in 30 voters willing to revote when they learned from the ESS PBC2100 receipt that they had spoiled their ballot. Consider that a person decides to commit fraud against a machine with a VVPT. Software could be designed to take advantage of the way voters seldom verify or, even less commonly, act on the information on paper receipts. If the software is designed to print the paper trail incorrectly, some will not notice that there is a problem. Additionally, a line of people will likely be waiting to use the voting machines, and the ballot workers are confronted all day long by people who consider themselves to be disenfranchised by the process so any genuine concern may not be addressed. In the first 10 minutes of watching people vote in LA County, I saw a person give up and decide not to vote because of the line and another person outraged by the procedure for voting when he was not found as a registered voter. Voters want to be helped inside the ballot booth. Voters want to take more time than allowed. Are poll workers able to distinguish these kinds of concerns and concerns stemming from a genuinely defrauded machine?

To defraud a VVPT machine a hacker might make the machine skip a race or appear to have a bad printer, perhaps by making the printer look like it's printing while it's not actually printing anything readable, or simply by making an unreadable section on the receipt. If this unreadable section is carefully printed it will be unreadable in a later recount. This could be used to cover up software defrauding of the electronic vote or it could hide changes in the vote inside the computer.

The vote inside the machine and the vote on the paper could be made to agree or disagree with the electronic vote. In making the VVPT and electronic ballot disagree, the defrauder could be calling into question the quality of technology to create a reason to call for a new election.

In a more likely scenario, the defrauder will change the electronic ballot and depend on the statistics for reading and contesting bad receipts. If a person calls their receipt into question and asks for another receipt to be printed, the hacked VVPT machine can print the "duplicate" receipt correctly, fixing the mistake. By printing the correct receipt when a person asks for it a second time it could literally eliminate the changed ballot, thus eliminating the possibility of detection. Although the program has to give up this one changed ballot it won't happen often. If this follows the experience described above, only one in three to one in 30 people that see a problem will be willing to do something about it. A hacker changing one percent of votes could count on between one in 300 and one in 3,000 voters who see a problem wanting to do anything about it. Considering that up to 1/3 of the fraudulent receipts would be noticed, the hacker has to change one in 75 votes to get a one percent change in the outcome.

If everyone reads their paper receipt carefully, one out of 225 people might notice that their paper receipt is different from their vote. The natural thing is to have the printer reprint it. In a precinct voting 500 people, this will be noticed twice during the day. When a voter complains and it comes to the attention of one of the several ballot workers that are running the election in a balloting area, it is likely to be caused by the ergonomic problems described above.

If it is because of the fraudulent VVPT, it will likely be the first time the ballot worker encounters this problem, which will make it harder to handle correctly than if they encountered it often. They are likely to encourage the voter to reprint the receipt that would, as outlined above, allow the voting machine to fix the internal count and print the correct receipt to cover up the fraud. If the ballot worker does enter the balloting area where the voter is, in order to verify the legitimacy of a problem with a VVPT, then they would have compromised the secrecy of that ballot. Even if they did enter the voters balloting booth to observe the strangely printed receipt, the natural reaction to an unreadable receipt would be to print a duplicate receipt themselves. Exchanging printers would also reprint the ballot, thereby eliminating the

evidence. Shutting down the machine is the only thing that would preserve the fraud to view later, but this would disenfranchise other voters.

As described above, a printer can fake printing problems to cover up changes to the electronic and physical records. By doing this, it can introduce fraudulent tallies. Another way for software to defraud the paper trail is to print more receipts than voters. This could easily be seen as a mechanical problem at the time.

### **Mechanical problems with VVPT**

Voting experts have been concerned about VVPT printers having problems. For instance, the connection between the printer and the machine can be broken, which would stop the printer functioning, and would keep people from being able to vote. If the printer were in the same unit as the voting machine, this problem might be lessened. Unfortunately, that would mean that the voting machine itself would have to be serviced to service the printer. Still it is a separate subsystem and would reduce voting machine reliability.

A printer can break mechanically—the motor, the levers or the solenoids can stop working, for instance. A plug replacement printer could be available, but the problem with the plug replacement printer is whether or not it can pick up where the other one left off. Has one ballot been lost in the meantime? Are we inserting a ballot accidentally when installing a printer? The person replacing a part can read the receipt because it is voter-verifiable. If they do change the paper, do they have access to the printout?

Additionally, the ink can be dried up or run out. If all printers are given new supplies preceding the election and tested, this should not be a problem. However, ensuring that such procedures include signoffs and checks of ink expiration dates is crucial to eliminating ink problems. If the printer is thermal (as many voting equipment printers are), the ink can't dry out. The problem with thermal devices is that heat applied to the paper before or after the election can destroy the printing. Thermal printing also fades with time and the paper tends to deteriorate more quickly.

These issues of printer failure might seem to be minor, but when considering LA County in which 2.2 million people vote in one day, the implications of mechanic problems that can occur are gigantic. In order to add any system that will not increase spoiled ballots, it must not add errors to the system. For the additional paper receipt to complicate the voter experience it must not misprint, jam, run out of paper or ink, malfunction, break, or lose its connection in a way that compromises the secrecy, integrity or accuracy of the vote.

To not lose votes, the printers must be shown to be able to print without failure during a voting election. Each printer must be able to print a typical precinct ballot every election for its planned lifetime. The number of voters in a precinct would not likely be more 200 voters per machine per election. General and special elections typically occur not more than 5 times a year. If the printer is to be used for 10 years a calculation of 15 years of life gives that it should be able to print 15,000 ballots without breaking.

The chance of breaking as opposed to wearing out is different; no machine should break down the day of election in a way that could lose a vote. For LA County, printers would have to have a reliability test that would ensure that they have a mean time between failures that is much larger than 2.2 million.

### **Alternatives to VVPT**

The possible means of improving the authenticity and reliability of software are many. First, better methods for better software development can easily be applied to voting. Modular architecture that separates the different parts of the machine and makes it possible for them to be tracked separately is a good approach. Encrypted votes could improve the validity of the system. Allowing everyone to view the computer program as “open source” is a fashionable approach to ensuring that simple problems in it are not evident.

The “votometer,” is a separate system that allows the voter to observe the vote without changing the software. To the extent that a votometer is written by a separate set of people that have no communication with each other, they cannot be in conspiracy to defraud votes. This separate verifying computer can also present the data in exactly the same format as the voting machine. This allows people to compare their votes with a record of those votes in the same format. It can be enhanced by special optics that overlay the two images of the two different displays. Such a votometer system can easily be verified and work across disabilities. The most exciting improvement of votometer over verified paper trails is that reading it is easy, doing it is easy, and establishing its separateness is easy. By solving all of these problems the votometer can literally eliminate the problems of setup and teardown. It can recognize the problems of voting, and establish authentic and separate verifications of the ballot.

Another verification approach is Voter Verified Audio Transcripts (VVAT), which speaks the names of the selections into earphones as selections are made. One advantage of this system is that receiving feedback while a person is making selections is easier to verify than a ballot later. Also, the tape that it produces is easy to count and has better integrity than receipts in a ballot box. Such a system can be implemented with the audio hardware available in today’s DRE voting machines.

In the future, many other approaches for establishing verification and audit of votes are possible. Systems could have multiple pieces of software checking each other or multiple computers could verify each other’s results. The most exciting of these is a voter's ability to compare his or her vote with the vote stored in the database of the government before they leave the voting booth. This will, in fact, some day be possible. When this is possible not only will we have a qualified belief that the vote this person cast is the vote that is stored in the computer, but we will also have deep security and the knowledge that what occurs at the very front end of the computer in establishing voter intentions is carried through, not only from the registration and authentication, marking the ballot, recording the ballot, storing the ballot, but also to recording the ballot in the election as it is being counted.

We can begin by verifying the votes on parallel machines. Parallel voting consists of pulling a voting machine out of service at random and assigning it to a phantom precinct. By controlling the votes that are cast and checking the results it collects, the machine can show that it recorded them as they were cast, ruling out an extra computer program, a “Trojan horse”, “Easter eggs” or other fraud. The voting machine is then used in a real election as a test of its ability to count votes correctly on the day of election thereby establishing the quality of the machines.

## **Conclusions**

This paper shows there are many different ways of disenfranchising a person using a voter-verified paper trail. First, people can be disenfranchised in all the normal ways. They can have registration problems; they can have valid design problems, polling place problems, etc. Second, the paper trail can be lost, stolen, or added to. Third, the equipment can be designed or accidentally set up so it doesn’t work, or it slowly changes itself. Finally, intentional fraud can be widespread and created in software in such a way that it can be hidden from the voter and from the ballot worker on the day of election and not be remedied later. The final problem is that counting paper cannot be done at the accuracy level that electronic counting can be done. In this way, even if everything is performed correctly, the difficulty of counting the paper electronically will make it impossible to compare electronic outputs with the paper outputs in a way that can determine whether an accurate count has been achieved.

The Voter-Verified Paper Trail discussion has diverted attention from the main sources of lost votes in past elections. The majority of votes are lost because of problems of registration databases, ballot design, and polling place operations. The force of this discussion is even diverting voting technology development away from improving voting computer architecture. The Voter-Verified Paper Trail has blocked us from establishing standards for improving voting equipment.

Furthermore, VVPT complicates two of the top three problems that have compromised more than one percent of American votes in 2000: equipment problems and polling place operations. It complicates the setup, teardown, and operations of the ballot place. It complicates polling place procedures during the vote. It gives extra and difficult tasks for a person to do and increases the problems with the user experience and the user interface. It also increases the length of time of voting, which makes it, with more steps, easier to make mistakes.

The goal of Voter-Verified Paper Trail—that of establishing a second set of eyes to look at the intentions of a voter—is a worthy one. In fact, ballot design and voting have always been improved by more people looking at the process. In every case improvements in voting have occurred when one person cannot make a decision that changes the vote of another. The idea of establishing a way of doing that is valuable.

We call for improved research in voting technology and for heightened concern over spending large amounts of money on a short-term solution to software hacking problems that have not yet surfaced in elections. Instead, let us focus on verifying the votes in many ways and improving the quality of the whole system.

### Citations and References

1. Michael R. Alvarez, Steve Ansolebehere, Erik Antonsson, Jejoshua Bruck, Steve Graves, Thomas Palfrey, Ron Rivest, Ted Selker Alex Slocum Charles Stewart III, Voting - What is, what could be., Caltech/MIT voting project, July 2001
2. Eric Fischer, Election Reform and Electronic Voting Systems (DREs); Analysis of Security issues: CRS Report for Congress, Order Code RL32139 Congressional Research Services Library of Congress, November 4, 2003. <http://www.epic.org/privacy/voting/crsreport.pdf>
3. <http://fecweb1.fec.gov/hava/hava.htm>
4. Roberta Klatsky, Human Memory Structures and processes, Second Edition, W. H. Freeman, San Francisco 1980,
5. Rebecca Mercuri, “A Better Ballot Box?” IEEE Spectrum, Volume 39, Number 10, October 2002.
6. Roy G. Saltman, Accuracy, Integrity and Security in Computerized Vote-Tallying, National Bureau of Standards Special Publications 500-158, August 1988.
7. Roger N. Shepard, Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior*, 1967, 6, 156-163. (a)
8. Michael Tomz , Robert VanHouweling, “How Does Voting Equipment Affect the Racial Gap in Voided Ballots? *American Journal of Political Science* 47, no. 1 (January 2003): 46-60.