

Paper v. Electronic Voting Records – An Assessment

Michael Ian Shamos¹
School of Computer Science
Carnegie Mellon University
April 2004

Abstract

There has been much discussion in the popular press concerning the use of contemporaneous paper trails to plug various perceived security risks in electronic voting. This paper examines whether the proposed paper solutions in fact provide any greater security than properly maintained electronic records. We conclude that DRE machines pose a number of security risks but that paper records do not address them. A number of alternatives to paper trails are suggested to respond to DRE security concerns.

1. Introduction

Among the arguments that have been advanced against the use of direct-recording electronic (DRE) voting systems are the following:

1. Voting machines are “black boxes” whose workings are opaque to the public and whose feedback to the voter is generated by the black boxes themselves. Therefore, whether or not they are operating properly cannot be independently verified and the machines should not be used.
2. No amount of code auditing can ever detect malicious or even innocently erroneous software. Therefore the machines should not be used.
3. No feasible test plan can ever exercise every possible combination of inputs to the machine or exercise every one of its logic paths. Therefore the machines should not be used.
4. Hackers can break into the FBI’s servers and deface its website. It ought to be child’s play for them to throw an election. Therefore the machines should not be used.
5. DRE machines have been plagued by a host of failures all around the country. Therefore the machines should not be used.
6. The DRE industry is dominated by a small number of companies, some of whose executives are announced supporters of the Republican party. An executive could command his programmers to add code to each machine manufactured by that company to move votes to a favored candidate, thus determining the outcome of the election. Therefore the machines should not be used.
7. Many prominent computer scientists have said that DRE machines cannot be trusted. Therefore they should not be used.
8. If added to a DRE machine, a voter-verified paper trail allows the voter to satisfy herself² that her voting preferences have been recognized correctly by the machine. Therefore, the voter-verified paper trail solves every one of the aforementioned problems and every DRE machine should be required to have one.

Each of these arguments will be examined in this paper and found fatally flawed, at least to the extent that it implies that machines cannot be relied upon to count votes in real elections. The numbered statements above all share the property that the first sentence of their premise is true, yet their consequent, that DRE machines should not be used, does not follow from the premise.

In 1993, I prepared a paper for the Computers, Freedom and Privacy '93 conference exploring the risks of electronic voting³. Since then, I have often been asked whether I still adhere to the opinions expressed in that paper in light of the incidence of widespread hacking, Internet worms and viruses, new cryptographic attacks and the increased use of DRE machines around the world. The answer is that I still hold those opinions but feel compelled to update the justification for them to respond to the arguments raised above.

Since the Industrial Revolution, man has chosen to rely on machines for tasks that are either impossible for humans to perform, or so expensive or repetitively boring that there is no justification for continuing to waste human labor on them. Many of these machines, such as cars, airplanes and therapeutic radiation equipment, among numerous others, have the capacity to take human life. They also commonly contain embedded computer systems. In the business world we rely on computers to execute financial transactions totaling at least \$2 trillion per day. It is well-known that all of these systems present risks. There are approximately 40,000 deaths annually in the U.S. due to automobiles⁴; some number of the victims are killed by malfunctioning software rather than human error. People have also been killed by the computer programs that control radiation machines⁵. In light of such failures, why do we continue to drive cars, fly on planes and receive radiation treatments? Why hasn't the government outlawed these killing machines?

The reason is that testing and safety procedures are in place that reduce the risks to levels that are deemed acceptable. There is no basis for applying different reasoning to voting machines. Once we decide what a tolerable risk in such systems might be, we can require that the equipment meet that standard. Perfection is never required, expected or even possible in any real system, though it is a laudable aspiration, and perfection is not required, expected or possible in voting systems, either. Federal Election Commission Standard 3.2.1 allows a maximum error rate of 1 in 500,000 voting positions⁶. With a typical ballot size of 235 positions, this is an allowed error of almost one in every 2000 ballots, or 0.2% of the vote.

When the safety procedures are found to have flaws, the flaws are ultimately corrected because of public pressure, government mandate or the relentless law of the marketplace. We are now seeing immense public pressure being put on voting machine manufacturers, along with threats to legislate, both of which are appropriate.

A secondary reason that machines presenting some risk of injury are not outlawed is that people generally have the option not to use a particular machine. This choice is also available to a voter, who may eschew voting machines completely and cast a paper absentee ballot.

While the United States has been using direct-recording electronic voting equipment for well over 20 years without a single verified incident of successful tampering, within the last year a number of people knowledgeable about computer security have questioned whether certain DRE systems in current use are sufficiently secure to be employed safely in elections. Some criticism of these systems resulted from examination of their source code, perceived flaws in their handling and use or from consideration of purely hypothetical scenarios. A calm observer

might take solace in the observation that if DREs are so dangerous, then surely at least one security hole would have manifested itself by this time. Realistically, however, hacking has been advancing at a alarming rate, and new attacks are constantly being discovered, so we are entitled only to a small bit of comfort from DRE history.

It is an error, though, to ascribe to DREs generally the bad attributes exhibited by some of them. The spectrum of available systems is broad. Some machines are excellent, some are terrible.

1.1. The “Black Box” Phenomenon

That a machine contains a computer and the computer contains object code not readily viewable or understandable by the public is by itself no reason not to use the machine. If it were, no one ought to own a personal computer. Neither passenger nor pilot can see or understand the software that operates the control surfaces of a jet plane. Such software could contain code, malicious or otherwise, that might send the plane into a dive at noon on a specific date from which the pilot could not recover. How do we know for a fact that such code is not present? We don't. Yet pilots and passengers continue to board planes every day. Let's look carefully at the reasons we allow jets to operate. All of them apply to voting systems as well.

1. It is beneficial to aircraft manufacturers to make safe planes. Planes that crash will not sell and will eventually be outlawed, not to speak of the legal liability associated with such incidents. This benefit induces the manufacturer to develop internal procedures designed, but not guaranteed, to produce safe products. It is beneficial to voting system vendors to make safe systems also. Whether they know how to do so, or have successfully implemented procedures for doing so, is somewhat questionable. In examining more than 100 different voting systems for certification purposes, I recommended that over 50% of them be denied certification. The quality and reliability of particular DREs is certainly a matter of concern, and later in this paper various solutions will be suggested.

I have heard it expressed that it might not be beneficial under certain circumstances for a voting system manufacturer to produce an honest machine, but that substantial gain could be achieved by distributing machines or software altered to cause the election of specific persons who may not actually be favored by the electorate. We will discuss below the practical difficulties with such a scheme, but if a manufacturer felt that its underhanded activities would not be discovered, such a fraud might be attempted despite the possibility of severe criminal penalties⁷. Therefore any plan for the administration and use of voting machines should contain safeguards against this type of manipulation.

2. Planes are built to high performance and engineering standards. Agreed. Voting machines, which are far simpler than airplanes, can be (but are not always) built to even higher performance and security standards.

3. Planes can be tested. So can voting machines. Neither needs to operate perfectly. Planes shouldn't crash much and neither should voting machines.

4. If a plane crashes, we'll know about it. The significance of this statement, made by DRE opponents, is that we would then at least be able to take remedial action to prevent a recurrence, a fact of little consolation to the victims' relatives. The argument is made that election can be stolen under our very noses and no one would be any the wiser. But that ignores the real political fact that elections are local and local party operatives have an extremely

accurate sense of how the community is going to vote. The smell of irregularity is sufficient to set off alarms resulting in investigations and recounts. DRE opponents claim erroneously that in a disputed election there is nothing useful left to recount since all the records that remain were made by the malfunctioning machine. But this argument is wrong because the software that was used in the machine survives. (We can deal later with the assertion that the software might modify or delete itself to evade discovery.)

5. The people who fly airplanes have a vested interest in their safety. The people who run voting systems are likewise committed to clean elections. Pilots have been known to crash planes deliberately and election officials have been known to manipulate votes. Safeguards need to be built in to prevent both of these efforts from succeeding.

In short, I am unable to discern any engineering difference that allows us to entrust our lives to aircraft but would impel us to avoid voting machines. Not to endorse questionable voting systems or trivialize the possibility of chicanery, but I believe I and the republic will survive if a president is elected who was not entitled to the office, but I will not survive if a software error causes my plane to go down.

1.2. Computer Security

It is pointless to discuss the security of a computer system in the absence of a well-articulated list of threats. So let's enumerate and deal with them in order.

1. Isolated attacks on individual machines. There are any number of ways of interfering with the operation of any computer system, such as pounding on it with a sledge hammer or the slightly more sophisticated technique of exposing it to several watts of radio-frequency emission. Such efforts fall into the class of mischief rather than tampering because they cannot be used to cause a predetermined result.

A different form of attack is to gain access the hardware or software of an individual machine or small number of such machines and alter them, either by connecting to ports and interfaces or by opening the machine by force or with the help of an insider who may have the keys, along with manuals, plans and source code listings for the machine. It should be obvious that no machines should be used that allows any voter to connect to it electrically to during an election and any device that permits this should be decertified immediately. The question is how to prevent people from modifying the machines offline or at least to be sure the tampering will be detected before the machines are used.

One solution is to ensure that all software needed to operate the machines, including the operating system, is not installed in the machine until election day. The authorized, certified software, distributed from a central authority (not the manufacturer), can be brought up at the time the polls are opened. In this way no advance modification of any software would be fruitful. If it is deemed undesirable to do a full machine boot, a portion of the code can be loaded on election day and verify through message digests and encrypted checksums that none of the prestored files has been altered.

2. Attacks by hackers or insiders at a polling place. The tendency to use networked voting machines at polling places for ease of administration also increases the risk that an insider could use a computer connected to the network to distribute malware to the voting machines after the election has begun. The miscreant would presumably remove the malicious code or restore the original at some time before the end of voting so that no trace would remain of the

misdeed. This sort of attack presupposes that the insider is able to erase evidence of his deed during the election, for if the altered software is still present in the machine at the close of polls it can be detected. It also is a highly localized manipulation that affects the results at a single precinct only.

3. Attacks by hackers or insiders at a central count facility. Now the magnitude of the problem grows because the number of votes that are potentially affected can be extremely large. There are 35 counties (out of a total of 3170) in the United States with populations exceeding 1 million⁸. The total population of these counties is over 73 million, approximately 25% of the country's population. A successful attack on central count systems in these 35 counties, (representing just 1.1% of the total number) would certainly influence any election, so every step must be taken to prevent such an event. Fortunately, in most states the results produced at central count stations are informational only, and are not the official election returns. With DRE systems, the ballot images representing individual voters' choices are stored both in the machine on which they were cast in redundant memories and also in removable modules that can be transported. All of these memories are cryptographically linked so substitutions and cracking are not feasible. A manipulation of the central count computer would not be to any avail since the totals produced there would not correspond to the canvass of individual precincts.

4. Insertion of malicious code by the machine manufacturer. There are two subcases. In the first, the manufacturer delivers software to a jurisdiction with prior knowledge of the ballot layout, candidate names, etc. for each precinct in the jurisdiction. The machine is programmed to behave perfectly before and after the election but to switch votes to favored candidates during the election. This manipulation is possible if the manufacturer is able to distribute software directly to specific precincts prior to an election. Countermeasures are discussed in sections 3.5 and 3.6, below.

In the second subcase, the manufacturer has no foreknowledge of the details of any specific election but distributes master software that causes candidates of a particular party to win in all future elections. The practical possibility of such a scheme is nil. There are about 170,000 election precincts in the United States. It is not possible to move a constant fraction of votes from one party to another in each jurisdiction without it being obvious that manipulation is going on because the political demographics of the precincts are too individualistic and distinctive. Therefore the software would have to be distributed with a database telling it how to alter the vote for each relevant candidate in each precinct. The database would have to contain at least the names of political parties and possibly candidates and would have to know in advance the precise hours during which all future elections are to be conducted so the machine would know when to behave properly.

This nightmare scenario, in which a small number of programmers manipulate the politics of the United States by injecting undetectable malicious software into voting machines has more in common with spy novels than it does with reality. For example, in the movie *Goldfinger* (1964), a crazed collector of gold apparently uses nerve gas to kill the entire garrison of troops guarding Fort Knox, then enters the vault where U.S. gold is stored and almost sets off an atomic device that would render the U.S. bullion supply radioactive and useless, which would immensely increase the value of his own holdings. When the film appeared, did the Army close Fort Knox out of fear that the plot was realistic? No. The reason is that adults eventually develop the ability to distinguish fact from fiction, a critical intellectual facility that should not

be abandoned simply because we are talking about voting. Did the Pentagon evaluate the plot to determine whether there were security weaknesses that ought to be remedied? Probably. Were some security procedures modified to reduce the probability that such a plot would succeed? Maybe. Is breaking into Fort Knox in such a manner absolutely impossible? No. Why, then, if there is some nonzero probability that a person could do it, do we allow our gold to remain stored there? It's because we never require perfection in real systems. We balance the risks rationally against the cost and other detriments of preventing the risks and make a reasoned determination. Just because a novelist (or a computer scientist) can dream up an entertaining doomsday plot involving voting machines does not mean we should toss them on the junk heap.

The argument I have with DRE opponents is that they insist that any conceivable risk of any kind of manipulation is unacceptable. That standard is never applied anywhere in human affairs, and there is no reason it should apply to voting, despite appeals to patriotism and pious claims that our very constitutional system is in jeopardy.

I do not propose that machines or software ought to be trusted just because they use advanced technology. In his 1984 Turing award lecture, entitled "Reflections on Trusting Trust," Ken Thompson demonstrated a method of hiding malware so it absolutely cannot be detected by any amount of examination of the corresponding C source code⁹. The technique involves corrupting the C compiler so that it recognizes certain patterns in the source program and compiles them into object code that performs not as written but as the malicious intruder intends. Of course if one is able to modify the compiler in this fashion the compiler could just substitute an entire program of its own choosing upon reading a "signal" string in the source text. Efforts to test the compiler to reveal its misbehavior would be frustrated unless one knew the signal string, since if the string were missing the compiler would always perform properly. Theoretically this hack enables arbitrary amounts of code to be inserted into any program at the cost of introducing but a short sentinel string to tell the compiler to start its dirty business.

The Thompson Trojan horse is frequently cited by opponents of electronic voting¹⁰ as a reason not to rely on voting machines. No one has ever suggested a remotely practical manner in which the world's compilers could become corrupted, but let's assume there is some way of sneaking a rogue compiler into a huge number of computers. This ignores the fact that jurisdictions themselves do not compile voting software, and that even though the source code may not be revealing, the object code contains all the evidence necessary to detect the intrusion. A decompiler can be used to verify that the malware is not present and/or that the object code being used corresponds to the original object code.

The argument has even been made that Turing's proof of the undecidability of the Halting Problem has some applicability to DRE machines¹¹. The cited paper asks us to draw the conclusion that "Determining that software is free of bugs and security vulnerabilities is generally impossible." That statement is true only if the word "generally" is carefully defined. A correct version of the statement, but one unsuited to the opponents' purposes, is "There is no procedure that is always *guaranteed* to determine whether an arbitrary program is free of bugs and security vulnerabilities." The unsolvability of the halting problem does not imply that no program can be proven correct, nor does it imply that the halting problem for restricted programs is unsolvable. For example, FOR-loops that do not modify the index variable or its limits and contain only straight-line code do halt. These are precisely the type of loops that are used for iteration in vote tabulation.

Assuming that one believes it is necessary for voting system vendors to produce mathematical proofs that their software is correct (an unreasonable proposition), one can easily imagine structuring a program that reads a finite number of ballot images and produces vote totals to be amenable to such a proof. I therefore must brand references to undecidability in the context of electronic voting simply as sophistry.

1.2.1. The Omniscient Hacker

Combining the misleading Halting Problem argument with the Ken Thompson code-hiding method produces a fantasy that I refer to as the “omniscient hacker,” which was explained to me by an opponent of DRE machines who will probably be grateful not to be named here. The hypothetical omniscient hacker is able to insert arbitrary amounts of malware into a voting system in such a way that it can never be detected by any amount of code reading (source or object) or testing (before, during or after the election), yet is able to alter the votes to achieve any predetermined result in any jurisdiction for an arbitrary numbers of years into the future. We need not yet go into the details of why such a thing is or is not possible, since a moment’s reflection reveals such a hypothesis to be no more than a purely religious belief. By the very premise of the statement the malware cannot be detected, so no amount of evidence of its non-existence can disprove the statement. If the malware ever is detected, the hacker will explain that he just didn’t do a good enough job hiding it, but he’ll succeed the next time. In this way belief in the omniscient hacker is indistinguishable from belief in a Supreme Being. There is simply no argument one can give that will dissuade a true believer, yet when the believer is asked for a demonstration he is unable to produce one.

That said, here is an adversary argument that demonstrates that the omniscient hacker cannot exist, though for the reason just stated I do not expect true believers to accept it. If we test the machine during the election by feeding it votes in a manner indistinguishable from regular voting, the malware must decide whether it is going to tell the truth or lie about the vote count. If it tells the truth, it has disabled itself and we need not be concerned that it is present. If it decides to lie, we will catch it, since we are casting a set of ballots whose totals are known.

It is of course possible that there are ballot combinations we may not have tried that will cause the malware to enter lying mode, but there is little risk that ordinary voters will happen upon those combinations either and the malware is either effectively silenced or it will be caught. One can imagine a magic input to the machine that will cause to begin lying (such as writing in the name “Turing” for President). But then activating this feature on every voting machine, or even a substantial number of them, would require a conspiracy of huge proportions.

By its very definition there can be no defense against the omniscient hacker, since we would never be able to tell whether he has been thwarted. (We might as well postulate the existence of an omniscient tamperer who is able to substitute an arbitrary number of voter-verified paper trails without detection. There’s no defense against him, either.) Belief in omniscience is a matter of faith. Those who really accept the possibility of an omniscient hacker will never be satisfied with DREs.

1.3. Voting Machine Standards

Since 1990, the Federal Election Commission has developed and promulgated Voting System Standards¹². The current version of these standards is now several hundred pages long.

They deal with hardware, software, telecommunications, security, qualification, testing and configuration management, among other issues. They are voluntary in that any state may, but is not required to, adopt the standards as part of its voting system certification process. As of this date, 36 states and the District of Columbia have done so. The standards are clearly a step in the right direction and obviously enjoy widespread state support, although one wonders whether the states have really evaluated the standards and found them to be meritorious or have adopted them for convenience. It is difficult, however, for a standards-making body to keep up with developments in computer security, develop countermeasures for newly-recognized threats and document them in the form of precise standards. Thus Volume I Standard 6.4.2, entitled “Protection Against Malicious Software” is just two sentences long: “Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.” An Independent Testing Authority (ITA) would be justified in claiming that the standard gives no operational guidance in testing a system to see whether it is secure against malicious code. It also appears to pass the burden to vendors, who are the very parties against whom we seek protection.

Independently of the FEC Standards, Section 301 of HAVA¹³ purports to impose certain minimum standards on “each voting system used in an election for Federal Office.”¹⁴ The term “Federal Office” is not defined in the statute but the Department of Justice takes the position that it has the meaning defined for it in other Federal election statutes, namely, “the office of President or Vice President, or of Senator or Representative in, or Delegate or Resident Commissioner to, the Congress.” Laying aside for a moment the question whether Federal control of Federal elections is a good or bad thing, Section 301 of HAVA is unconstitutional on its face. While the Congress may make rules concerning elections for senators and representatives¹⁵, it has no power to specify standards for presidential elections. Article II, Sec. 1 of the U.S. Constitution reads in part: “Each State shall appoint, in such Manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the State may be entitled in the Congress ... The Congress may determine the Time of chusing the Electors, and the Day on which they shall give their Votes; which Day shall be the same throughout the United States.” Thus Congress has no power to determine the manner in which presidential electors are chosen other than to specify the time and date of their election.

No one seems to have noticed this unconstitutionality, but more probably the states simply do not care, since HAVA allocates billions of dollars to them for acquisition of voting machines – a case of not acknowledging that the gift horse even has a mouth. In any case, HAVA does not deal at all with the problem of malicious software.

1.4. Testing

DRE opponents argue that DRE software may contain up to 50,000 lines of poorly-written code that is impossible to read or test¹⁶. The argument is misleading – deliberately so in the author’s opinion. It is true that complete voting software systems, including ballot setup and printing components, may reach that size, but the portions of code that accept input from the

voter and record ballot images – the very portions suspicions about which have given rise to calls for paper trails – are tiny by comparison.

While it is surely true that not every logic path of a computer program of any size can be exercised, this is obviously not a reason not to use software. Otherwise no commercial software would ever be used, and surely not in any situation in which human life were at risk. The issue is whether any combination of code reading, program testing, open source code publication and other techniques can give us adequate assurance that the software does not contain malicious code or logic errors that will cause votes to be altered. The answer is certainly yes. If code is too obscure, or contains portions that are not readily understandable, it should not be used. Only if the relevant programming is transparent and available to the public should we be confident about using it.

One should realize that the basic loop that interrogates portions of a touchscreen and interprets them as votes is not very complex, although an entire election administration system might be. When the user touches the screen the processor is notified through an interrupt and receives the geographic coordinates of the point that has been touched. A search is made to determine which box on the screen has been touched. Any code that is present that treats candidates differently based on their ballot positions should not be there.

1.5. Machine Failure

By far the most justifiable criticism of DRE machines is that they fail during service or in some cases cannot even be brought into service on election day. There are numerous documented instances of such failures. These incidents are real. They are intolerable when they interfere with the act of voting.

It is important, however, to understand the nature of the machines' failure modes. They do not suddenly decide to move votes from Democrats to Republicans. They may "hang up," refusing to accept any more votes. The mechanical components, particularly the touchscreens, may develop dead spots or fail to register at all. Switches and buttons wear out. Circuits exhibit erratic behavior. These situations can result in severe voter inconvenience and loss of confidence in the process. Long lines can develop, causing voters to balk and go home. The sight of technicians opening machines and replacing components in full view of the voters does not promote trust in the integrity of elections.

While voter inconvenience is certainly detrimental, the critical question is whether any votes are actually lost or modified when the machines fail. In properly designed DRE, no vote once cast is ever lost because ballot images are stored in redundant memories, including write-once devices. It is possible, however, for a machine to fail in such a way that votes cast subsequent to the failure are misrecorded. When the failure is discovered later, it may be too late to reconstruct the lost votes. This situation is akin to mechanical failure of a lever machine – regrettable, but not fatal so long as the failure is not systematic or deliberately induced.

The matter of machine reliability is a question of design, engineering, testing and adherence to maintenance procedures. The responsibility of the vendor is not to be overlooked. A proper voting machine procurement will impose heavy penalties on vendors whose machines do not conform to warranty. If a jurisdiction is unwilling to rely on indemnification by a vendor, a solution is to acquire spare machines and stand ready to deploy them as needed during an election.

It is the author's opinion that many of the so-called failures of DREs in fact resulted from inadequate training of poll workers in using the equipment. HAVA has created an incentive for counties to rush to procure and begin using DREs. Some jurisdictions have done so without adequate preparation, and have seen failures occur during an election. When machines are tested at the warehouse immediately prior to an election and are found to be working, yet cannot be started on election day morning, it is much more likely that the problem results from unfamiliarity with startup procedures than a sudden and unexplained failure of the equipment.

Despite energetic efforts by opponents to slow their adoption, DRE machines continue to be adopted at a prodigious rate. India, the world's largest democracy with over 650 million voters recently adopted DRE machines nationwide. Just its 600,000 villages constitute more than four times as many election districts as there are in the entire United States.

2. Paper Trails

It has been asserted that adding paper trails to DREs allows prompt detection of all of the possible intrusions discussed above. It is based on the mistaken belief that paper records are in some way more secure or free from tampering than electronic ones, which is not the case.

On March 20, 2004, a presidential election was held in Taiwan. The winner by 29,518 votes (out of over 13 million cast) was the incumbent, Chen Shui-bian. To achieve this result, the Central Election Commission had to declare 337,297 ballots as invalid, more than 11 times the supposed margin of victory. The voting method was by paper ballot, and there weren't even any DRE machines to blame. Surely if the voters could rely on the paper ballots to be counted properly this result could not have occurred.

2.1. Paper Records

Humans have a profound affinity for that which they can see and touch. This results in a deep reverence for the printed word, whether it is true or false, and explains the comfort people derive from paper receipts. There are very few paper documents that have preclusive legal effect, meaning that the writing on the face of the document is not subject to challenge.

There are basically four types of paper records:

1. Bearer instruments. Examples: currency, bearer bonds, checks, movie tickets. Here the instrument itself entitles the bearer to rights with no further inquiry into his bona fides. Title to the document passes with possession. These instruments are extremely convenient for transactions because they can convey rights and title instantaneously without resort to offline records and databases. They are also a frequent subject of theft.
2. Receipts. Instead of being a instrument used to effectuate a transaction, a receipt is merely evidence of the transaction. As such, a receipt takes its place among all of the other forms of evidence, including spoken words, videotapes, witness testimony, business records, computer databases, etc. The receipt confers no independent rights, but is given for several reasons. First, a party to the transaction usually insists on a receipt (a) as evidence of the transaction, as in an ATM withdrawal; (b) to verify the correctness of its details, as in a restaurant bill; (c) as an aide-memoire to recall the transaction. It is used in the event of a dispute to lend credence to the claim of one party or another. The contents of a receipt may be challenged or rebutted and the effect it has will be determined by the trier of fact.

3. Business records. These are notes kept by a business as part of its operations. Records kept in the ordinary course of business are admissible as evidence, but they are only evidence and may be challenged. They differ from receipts in that they are created by one party to a transaction and but are not normally reviewed for correctness by the other party. A dispute between a bank and its customer over a questioned ATM transaction usually turns on the question of which records are more credible, the customer's paper receipt or the bank's computerized business records.

4. Ballots. A ballot is an expression by a person indicating how she wishes to cast her vote. A ballot is a unique document defined by election law and is itself only evidence of how a voter wanted to vote. A ballot may be challenged on many grounds, including an allegation that the voter was not entitled to vote, the ballot was mismarked, the voter voted in the wrong precinct, the voter cast votes for candidates she was not entitled to vote for, the ballot was mangled, defaced or was otherwise unreadable. In many, but not all, states when the content of a ballot is disputed, a court is required to determine the intent of the voter in marking the ballot and is not bound by that the ballot actually says.

There are numerous other forms of paper records, such as documents of title, licenses, wills, diplomas, written offers, etc., that are not relevant to our discussion here. The question is what desirable properties, if any, do paper records have that would cause us to prefer them over electronic ones for voting.

The largest industry in the world in terms of daily cash flow is foreign currency trading, which often totals more than \$2 trillion per day. The entire world securities industry rarely exceeds one-tenth of that amount, and no sector that deals in physical goods can even approach it. The vast majority of foreign currency trades are made without any use of paper whatsoever, either in the form of an original order or a generated receipt. If computers are unsafe and hackers and well-placed insiders lurk behind every door, one wonders why the traders don't lose a billion dollars a day (or at least a million) as a result of malware. In December 2003, no less a figure than Senator Hilary Clinton stated while introducing her "Protecting American Democracy Act of 2003"¹⁷: "You go to an ATM, you get a receipt. You play the lottery, you get a ticket. Yet when you cast your vote, you get nothing. The systems used by the people of the United States to exercise their constitutional right to vote should be as reliable as the machines people depend on to get their money. What's required for money machines should be required for voting machines." Statements that play well to the electorate often fail when subjected to the cool light of logic.

Sen. Clinton is correct that Regulation E of the Federal Reserve Board¹⁸ requires a financial institution to make a receipt available when a consumer initiates an electronic funds transfer at an ATM. She might be surprised to learn how limited the legal effect of the receipt turns out to be. If a financial institution fails to provide a receipt through "inadvertent error," it is not in violation of Regulation E¹⁹. Furthermore, the receipt itself is only prima facie proof (subject to rebuttal) that the consumer made a payment to a third party²⁰. It is not proof of the amount of transfer and is of course of no effect at all in the case of an ATM deposit, since the data associated with the deposit is generated completely by the consumer, not the bank.

In the event of a later dispute between the consumer and the bank, the ATM receipt is evidence only and is not dispositive of the question what amount was transferred. The bank may challenge the data on the receipt based on its own records. Note that the receipt has been in the

hands of the consumer and thus has been subject to alteration or forgery, which means that the document itself cannot be given absolute effect. Of course in electronic banking transactions initiated over the Internet there are no paper receipts at all, yet this fact has not dampened enthusiasm for online banking.

The law governing ordinary sales transactions, the Uniform Commercial Code, gives no legal effect to receipts and certainly does not require them²¹. In fact, neither party to a sale transaction has the legal right to demand a receipt, although it may be a customary business practice to comply with such a demand.

Sen. Clinton would be positively dismayed to learn that a lottery ticket has even less value to its holder than an ATM receipt. State lottery rules typically provide that if a dispute arises between the holder of a lottery ticket and the state lottery bureau, the computer records of the lottery bureau govern. This New Hampshire Lottery rule is illustrative: "To be a valid ticket and eligible to receive a prize ... [t]he information appearing on the ticket shall correspond precisely with the Commission's computer record."²² The lottery rules clearly provide that computer records govern over paper ones.

And so it must be. If presentation of a small piece of paper were sufficient to claim a prize of \$363 million²³, the inducement to fraud and bribery to produce a counterfeit ticket would be extreme, and the nature of paper is that it would be essentially impossible to invalidate the ticket based on a physical examination because genuine ticket stock can easily be obtained. This raises the question what the purpose of a lottery ticket might be if not to ensure the buyer that he will get paid in the event of a win. Despite what the public might believe, the lottery ticket is simply a receipt, that is, an item of evidence that can be considered in the event of a dispute. It also provides the buyer with the opportunity, in the act of buying a ticket, to verify that the human operator typed in his numbers correctly. The issue is not that the lottery ticket machine may have malfunctioned, but that the human seller may have made a mistake. (As we have seen, if the lottery machine malfunctions, that is, communicates a different set of numbers to the lottery commission than those printed on the ticket, the buyer has no effective recourse.) Because the only human in the voting booth is the voter herself, and the voter has ample opportunity to review her ballot, the verification function of the lottery ticket is not relevant to elections.

The lottery ticket also serves to remind the buyer which numbers he chose so he can later compare his numbers with the winning ones. It is also necessary to claim the prize, since a lottery ticket is anonymous and transferable. The state must know whom to pay. None of these considerations is applicable to voting²⁴.

Of course Sen. Clinton's Protecting American Democracy Act of 2003 is unconstitutional for exactly the same reason that Section 301 of HAVA is unconstitutional – it purports to allow Congress to legislate standards for presidential voting, a privilege reserved to the states.

When I raise the point to opponents of electronic voting that huge volumes of commerce are conducted based only on computer records, their answer is, "If anyone lost a billion dollars they would know. If someone steals votes, we'll never know." This explanation is appealing, but specious. If someone were able to manipulate a bank's computer records to spirit away a huge sum of money, it is reasonable to believe that he could do so while at the same time not only deleting any computer records of the transaction but also modifying the bank's records so it did *not* know there was any loss. But in any event it does not matter whether the bank knows

that it has lost a billion dollars or not – the money is gone and the risk the bank tried to avert has occurred anyway.

2.2. Electronic records

The areas of human endeavor in which electronic records are used in place of paper ones are far too numerous to list. Among them are banking transactions, income tax filings, medical diagnosis, military orders (including nuclear launch instructions) and securities purchases.

The public and the legal system have come to recognize that electronic records can be reliable if properly maintained. The Electronic Signatures in Global and National Electronic Commerce Act (“E-Sign”)²⁵ raises electronic records to at least equal dignity with paper ones. It provides that in “any transaction in or affecting interstate or foreign commerce ... a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.”²⁶ There are a small number of exceptions for such specialized documents as wills and testamentary trusts and notices of termination of insurance benefits, but otherwise electronic records do not have inferior status.

The regulations implementing the E-Sign statute generally provide that electronic records are equivalent to those on paper²⁷. The Uniform Electronic Transactions Act (UETA) has been adopted in 45 states and is pending the three others. UETA specifies the legal effect of electronic records and has as one of its stated purposes “to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions.”²⁸ If electronic records are questionable in some way, how has this fact escaped the vast majority of our state and federal legislators?

The Federal Rules of Evidence give equal weight to electronic records in court proceedings as they do to paper ones²⁹. It is therefore a puzzle why electronic records should be acceptable for every other government purpose except voting. Neither E-Sign, UETA nor the Federal Rules of Evidence contain any receipt requirement.

2.3. Paper ballots

Paper ballots can be divided generally into those that are intended to be read and counted by humans, which we shall call Australian ballots to avoid ambiguity, and those intended to be counted by machine. The latter included punched-card and mark-sense (optical scan) ballots.

Every form of paper ballot that has ever been devised can and has been manipulated, in general with considerable ease. The reason is that humans are familiar with paper and its characteristics, how to mark it to look genuine and how to erase it. Likewise, the number of people in the U.S. capable of producing professional printed matter is huge. There are over 50,000 printing companies in the U.S, employing over 1.2 million people, of whom more than 100,000 are prepress operators³⁰. This means that it is not difficult to locate people who can print or modify documents.

Other types of manipulation, such as destroying ballots or substituting other ones, require no skill at all. By contrast, altering redundant encrypted write-once computer records is impossible even for experts. So assuming that the electronic voting records are written correctly in the first place (a subject that indeed deserves discussion), the possibility of modifying them later is remote.

The simplest form of paper ballot manipulation is ballot-box stuffing, that is, inserting extra ballots, usually genuine ones that have been pre-marked, into the container meant to hold only those voted by registered voters. In any jurisdiction in which the voter can touch a physical ballot and personally insert it into a ballot box, she can conceal extra ballots on her person and insert them at the same time. This is true whether the ballots are Australian, punched-card or mark-sense. The practice is so widespread that many states have statutes specifically dealing with the situation in which more ballots are found in the ballot box at the close of voting than the number of voters who appeared at the polls that day. The Florida statute is both horrifying and amusing: “[I]f the number of ballots exceeds the number of persons who voted, as may appear by the poll list kept by the clerk and by the stubs detached by the inspectors, the ballots shall be placed back into the box, and one of the inspectors shall publicly draw out and destroy unopened as many ballots as are equal to such excess.”³¹ Yes, ballots are chosen at random and discarded until the totals come out right! The most appalling thing about the law is not how the procedure is to be conducted, but that the situation occurs frequently enough that the law had to be drafted in the first place.

Actually, the Florida process solves nothing except to avoid the unseemliness of having more votes cast than voters, which is always an embarrassment. If the ballot box has been stuffed, the random discard process will not alter the candidates’ percentages on average. That is, whoever wins by the stuffed vote total will probably also win after the excess votes are tossed away, and the stuffers will have achieved their objective.

Another form of manipulation is to perform substitution of ballots on a large scale. In central-count jurisdictions, ballots are not counted at polling places but are transported by vehicle to a centralized counting station, usually at the county seat. The ballots are carried in transport cases outfitted with locks and seals, but the locks can easily be opened and the seals counterfeited. It can take several hours in large counties for the ballots to reach the counting station, giving ample opportunity for chicanery. Instances are known in which manipulators did not even bother to open and reseal the ballot cases, but merely substituted others that had been prepared once the total turnout in each precinct became known. This sort of manipulation is made easy by the fact that printed Australian ballots are insecure and transport cases and seals easily obtained from unauthorized sources.

One of the oldest and easiest forms of tampering is to invalidate an Australian ballot while touching it. When I was in middle school during the 1950s, our American history teacher explained that poll workers would break off a piece of pencil lead and insert it under their thumbnail. When they found a ballot voted for a candidate they didn’t like, they would make a second mark for some other candidate in the same office, thus creating an overvote that had the effect of erasing the undesirable choice. Once this has been done, there is no effective way to reconstruct the original ballot.

Because Australian ballots have to be marked and read by hand, there is no real prospect for tampering to occur on a national scale. The same is not true of punched-card and mark-sense ballots. The only remaining use of punched cards in the United States is for voting, and only two manufacturers remain in the business. Without giving a catalog of possible tampering methods, there are many parameters in card manufacture than can be varied to the advantage of one candidate or another if the voting positions corresponding to the candidates are known at the time of manufacture.

The problem of hanging chads, long known in the election industry, came to public attention in Florida in 2000. But for years many states used “chad teams,” groups of poll workers whose function was to tear loose chads from ballots before they were fed into the card reader. Once we allow a person to alter a ballot that has been cast by a voter, anything is possible. A perfect tool for punching out chads by hand is the metal tongue from an ordinary waistbelt. Small and easily concealed in the hand, it can be used the same way the old pencil lead was employed to overvote Australian ballots.

With mark-sense ballots it is known that if the areas for marking the ballots are printed improperly or the timing marks at the side of the ballot are skewed, votes that are cast will not be read properly by the scanning machine. More tampering is possible through the selective application of inks that appear white but absorb the infrared light that is used in the reading process. An answer, one might think, is that we always have the original ballots around to recount by hand, but mark-sense ballots are just as susceptible to loss, substitution or augmentation as Australian ones.

In general, the rampant problems with paper ballots are neither acknowledged nor addressed by opponents of electronic voting, who seem oblivious to the fact that their opposition to new technology, if successful, will compel us to retain something that is much worse.

2.4. The “Voter-Verified” Paper Trail

It is alleged that adding a so-called “voter-verified paper trail” to a DRE machine will either permit tampering to be detected or at the very least will provide a reliable record of how each voter voted that can be used for a recount, even if the recount must be conducted by hand. This is incorrect. A paper trail accomplishes one thing, and one thing only – it provides assurance to the voter that her vote was initially captured correctly by the machine. This is no small accomplishment, but it can be achieved in numerous other ways, as explained below. That is the only voter-verified part. The paper trail provides no assurance at all that her vote will ever be counted or will be counted correctly. The reason simply is that the paper trail itself becomes insecure at the moment of its creation.

First, if the machine cannot be trusted, which is the working hypothesis of paper trail proponents, then it cannot be trusted to deal with the paper trail safely. After the voter leaves the voting booth, it can mark her ballot as void and print a different one. The voter will have left the booth believing not only that her vote was cast and counted properly, but that it will also be counted properly in any recount. None of these beliefs is correct.

One might argue that inspection and testing of the machine would reveal such abjectly bad behavior, but the claim of DRE opponents is that no amount of inspection and testing is ever sufficient. If testing is adequate to reveal paper trail flaws, then it is adequate to uncover other faults in the machines.

Here is a further, but only partial, catalog of problems with paper trails.

1. The paper trail cannot be on a continuous roll of paper, since that would permit reconstruction of each voter’s ballot based on the order in which votes were cast. Therefore, the paper trail must consist of separate pieces of paper. However, once the pieces of paper are separated, the integrity of the trail is lost. Looking at a piece of paper, we will not be able to tell for certain where it came from. Stuffing and all other paper ballot tampering methods then become possible. The addition of cryptographic indicia, which has been proposed as a method to

prevent insertion of unauthorized ballots, cannot work since the voter will never know whether her real ballot contained the proper indicia when it was created. If it didn't, the ballot will not be tabulated during a recount.

2. Adding a paper printing device to a DRE machine naturally adds another component that can fail, run out of ink, jam or run out of paper. If DREs are alleged already to be prone to failure, adding a paper trail cannot improve that record. In Brazil in 2003, where a small number of precincts had installed paper trails, failure of the printers delayed voters by as much as 12 hours, a figure that would be catastrophic in the U.S.³²

3. There is no voter-verified paper trail machine that has been tested on any large scale.

4. States that propose to implement the paper trail have promulgated regulations stating that the paper shall govern over the electronic record in the event of discrepancy³³. This has the effect of making the insecure paper record paramount over the secure electronic one, a return to the early days of the Australian ballot.

5. With complex ballots, voters are prone to forget exactly whom they have voted for. When confronted with a paper record, they may erroneously claim that the machine made a mistake. This will call the machine's reliability into question, prompt calls for a recount and cast doubt even on machines that are functioning properly.

6. Paper trails do not address the problem of DRE failures. If the complaint is that a machine cannot be initialized for use on the morning of election day, then having a paper trail mechanism is of no help. In fact, the presence of the mechanism increases the load on the machine's power supply and processor and itself increases the probability of failure.

7. The paper trail requires a re-examination of meaning of the terms "ballot" and "official ballot." This is not a mere semantic exercise, but a question of great legal and, in some states, constitutional significance. Can a piece of paper be a ballot if it is neither marked nor touched by the voter? If so, significant statutory changes will be required. If the paper is the ballot, then what conceivable meaning can be ascribed to the computer count, which is not derived by counting the "ballots," but by processing the voters' original inputs that were separately used to generate the ballots? If the paper ballots are official, then we are put in the untenable position of having to certify an election without ever actually counting the ballots, unless an allegation of irregularity compels a "recount."

8. Each losing candidate will claim that the election was stolen from him by the machine and will insist that the only true indication of the voters' preferences reside on the paper, even if there is no evidence of irregularity or tampering. Thus paper recount will become the default method of vote counting, mitigated only by the high cost of such recounts. If this is to be the case, why use voting machines in the first place?

9. Paper trails cannot readily be viewed by disabled voters, requiring them yet again to reveal their votes to strangers in order to have them verified. It is no answer to say that there are other mechanisms to review their votes. If paper trail proponents truly believe the paper trail is necessary for fair elections, then elections will not be fair for the disabled.

10. A report of the Caltech-MIT Voting project concluded that the presence of paper trails actually decreases public confidence in the voting system³⁴. This can be understood as follows: would requiring airplane passengers to inspect the plane's engines before boarding enhance their belief in the safety of the aircraft?

My position on paper trails, despite their problems, is not an extreme one. If a manufacturer produced a reliable paper trail device and the remainder of his system were acceptable, I would see no problem in certifying such a machine. I am firmly opposed to any audit trail requirement, however, and even where audit trails are used, the paper record should never govern over the electronic one because it is vastly less secure. The proper use of audit trails is as evidence. If the paper trail totals differ from the electronic ones, that is the starting point for investigation, not the end of the issue..

3. Alternatives to Paper Trails

If paper trails are not the answer, are there practical alternatives that will not only render DREs safe but also persuade the public that they are safe? Let us assume that all of the security risks discussed above (except the omniscient hacker) are realistic. Are there measures other than paper trails that will prevent them? The author does not discount the importance of assuring the voter that the machine is working and that her preferences have been collected without error. This can be done in a multitude of ways that do not involve paper.

3.1. Audit devices

A prime motivation for audit trails is the possibility that the machine has been programmed improperly, either by accident or by design, or that rogue software has been substituted for the authorized version. Suppose we were to require voting machines to be architecturally separated into two distinct devices: a panel, possibly but not necessarily a touchscreen, whose only function is to display the ballot and capture voter choices, and a tabulation and recording device, which accepts input from the panel and performs computations. The panels and tabulation devices could be supplied by different manufacturers.

Now suppose we feed the output of the panel to two different devices simultaneously. One is the tabulation machine; the other is an audit device made by yet a third manufacturer and programming by an independent body, such as an accounting firm or public interest group not affiliated with the tabulation manufacturer. The audit device displays the voter's choices on a screen of its own for verification. The voter views the audit screen, and if it is correct, presses a "VOTE" button. Both the tabulation device and the audit device make redundant read-only records of each ballot image. At the end of the election, all the records are compared. If they differ in any respect whatsoever, the results from that machine are called into question and an investigation is launched. An examination of the software installed in the two devices should reveal whose records are the reliable ones.

So long as there is no collusion between the audit device manufacturer and the tabulation manufacturer, no amount of tampering with either machine will go unremedied. The prospect of tampering identically with both, since their software systems would be completely different, is too small to consider seriously. The audit device could easily be outfitted so disabled voters could verify their votes.

3.2. Open source

The manufacturers of voting equipment claim that their software is a trade secret and go to extraordinary lengths to preserve that myth. The author has been looking at the source codes of voting systems for over 20 years and has yet to find any significant differences in their design

except possibly for the number of bugs they contain. They all do the same thing, albeit in somewhat different ways. No vendor's software is a significant selling point providing any competitive advantage over other systems – jurisdictions focus on the hardware. All the software has facilities for setting up elections, storing the candidate and party names in a database, presenting ballot choices to the voter, tabulating and storing the results and possibly transmitting them after the election. The systems vary in ease of use and capacity, but they do not contain trade secrets for the simple reason that every aspect of election setup and balloting is well-known to all.

One might speculate then on why they try to keep the source code confidential. The uncharitable view, which appears to have some justification, is that they don't want the public to see how bad their code is. A legitimate reason might be to avoid making matters easy for competitors, but that does not justify withholding information from the public that is necessary to promote confidence in the electoral process. Another reason is to hide security measures which, if disclosed, would provide a roadmap for hackers. I am somewhat sympathetic to that view, despite the meaningless but mocking phrase "security through obscurity," since I know a thief will have a much harder time stealing my car if he does not know where I have hidden the key than if he does, and a party who happens to find my hidden key will have no idea which car it fits.

On the other hand, there is no reason that the ballot setup, display, tabulation and reporting sections of voting system code should be kept secret, and manufacturers would be wise to accede to public demand in this regard.

3.3. Administrative procedures

The administrative procedures concerning the handling of DRE machines and materials are usually not spelled out at all, or, if spelled out, then not circulated and not followed. Many of the observed vulnerabilities in DRE systems stem not from problems of machine design, but from lax handling procedures. A thorough election administration manual should explain at least the following steps:

1. Custodianship of machines at all times, including transportation to and from polling places.
2. Receipt and registry of software to ensure that only authorized copies of everything, including operating system versions, are used in voting machines.
3. There should be no delivery of any software directly from vendors to jurisdictions; otherwise (2) will not be observed.
4. Deposit and security for ballot materials, including any election programming. Likewise, control of installation of election programming into voting machines.
5. Chain of custody for any removable media containing ballot images or vote totals.
6. In the event an audit trail is used, chain of custody for the paper ballot images.
7. Freezing of machines and their software at least until the election is certified and the time for any challenge has passed.
8. Exception procedures for handling irregularities during an election, including custody of partial totals on any machine that is removed from service.

3.4. Standards

It may not be fruitful to have all the states separately ponder and solve the myriad of problems in election administration posed by the sudden introduction of new voting technology. Knowledge and experience should be pooled and election officials ought to be able to rely on a full set of standards, including security and vote handling procedures, that they can follow. The FEC Standards were principally written for ITAs to follow, not for election jurisdictions, and do not specify processes that are responsive to numerous objections that have been raised to DRE voting.

The budget provided by HAVA is fully sufficient to fund development of a comprehensive set of standards and procedures which, if followed, would greatly diminish the number of problems observed at polling places.

3.5. Parallel testing

More than 15 years ago, in a Pennsylvania certification report, I wrote of the possibility that a DRE machine could contain an on-board clock and that an intruder could rig the machine so that it behaved perfectly in all pre- and post-election tests, but switched votes during an election. The prospect is even more real today than it was then, since computers now routinely possess such clocks. This attack presupposes that the software knows all dates and times for elections into the indefinite future, but let's assume it has such knowledge³⁵.

One solution is to forbid on-board clocks altogether, but that would limit various other capabilities, such as making a time-stamped record of happenings during the election. It also raises the question how one can tell whether a clock is present in a machine or not. The second obvious solution is to reset the machine's clock to a time on election day, run a test and then set the clock back to the correct time. This is ineffective since the machine could contain software that would detect such a change and know that it was being watched.

A better solution is to employ parallel testing, a plan originally suggested by this author that was used in 10 counties in California during the 2004 primaries. Under this method, a set of examiners is empowered to enter any polling place at the start of voting and commandeer any voting machine for test purposes. No actual voters cast votes on the selected machine. No change whatsoever is made to the test machine – it is not even moved from its position (to counter the argument that it might contain a motion sensor to warn that it was under test). The examiner votes a number of predetermined ballots comparable to the number that would be voted on a typical machine in that precinct. Of course, manual entry of votes by a human is an error-prone process, so a video camera is used to capture his actual vote entries. At the normal close of polls, the votes on the test machine are tabulated and compared with the expected totals. If any software is present that is switching or losing votes, it will be exposed.

The function of this test is limited. It of course does not ensure that even one other machine in the precinct is working properly. It is designed to detect the nightmare scenario in which some agent has tampered with every machine in the jurisdiction undetectably, a major risk cited by DRE opponents to justify the addition of paper trails.

The examiners would select precincts and machines at random on the morning of the election. It is an issue of statistical quality control exactly how many precincts should be chosen. This testing, while cumbersome, is much easier than statutorily mandated recounts in which a certain percentage of ballot images must be totaled manually.

3.6. Separation of candidate names

Perhaps the ultimate protection against malicious code is to keep candidate and party names segregated from the software so it cannot perform any meaningful manipulation. If the machine is programmed to move votes from one party to another, it will be stymied if it is unable to determine the party with which a candidate is affiliated or even which candidate is associated with a given ballot position. This can be done by presenting the candidate and party names and issue text in the form of graphic files that can only be read by a human being. The only thing the software can do is faithfully record the numbers of the ballot positions that were selected. Of course, since it also knows no candidate names, it can only report results by ballot position. To defeat such a countermeasure the software would have to contain a complete optical character recognition algorithm.

It is possible that in a conspiracy a tamperer's confederate could, while voting, provide information via touchscreen selections or the write-in panel that could inform the software of the particular voting positions to manipulate. However such an act would have local effect only, since it would take one confederate for each voting machine involved. It would not be feasible to perform manipulation on a large scale with such a scheme.

4. Answering the Objections

We are now equipped to respond to the objections to DRE voting raised in the Introduction.

Objection 1. DREs are black boxes. So are all other computer systems, on which we rely for our lives and our fortunes.

Objection 2. Code cannot be audited. Yes, it can. Not all code can be audited, and we can bar unauditable code from being used in elections. We can also make the code available for scrutiny by an arbitrarily large audience by making source code open.

Objection 3. Machines cannot be tested. Why not? Every other type of machine can be tested, and voting machines are not nearly as complicated as airplanes.

Objection 4. Hackers can do anything. Only in books and movies. The hacking stories we read in the papers concern attacks over the Internet against systems that are deliberately held open for access by the general public. Voting machines, by contrast, are highly controlled and cannot be accessed over the Internet. Hackers are not omniscient and even vendors have trouble programming tabulation software correctly. The prospect that a hacker could not only manipulate an election but do it without exhibiting a detectable bug is so far-fetched an idea that no one has come close to showing how it might be done³⁶.

Objection 5. DREs are failing all over the place. The answer here is simple: buy reliable ones. The FEC Standards specify numerous tests designed to weed out unreliable hardware.

Objection 6. The vendor can rig the machines. But we can expose him through any number of mechanisms, including audit devices and parallel testing. And we can render his manipulations fruitless by separating candidate and party names from the capture and recording logic.

Objection 7. Computer scientists say DREs are unsafe. Since when was this technological issue to be decided by popular vote rather than by analysis? There are over one million computer scientists and mathematicians in the United States³⁷. About 100 of them have

signed a resolution in favor of paper trails proposed by www.verifiedvoting.org³⁸. No information is available on how many have any familiarity with the processes of voting or the actual architecture of DRE machines, but the total number represents about 1 in 10,000, a minuscule proportion. The good news seems to be that the other 9,999 out of 10,000 have remained open-minded on the subject.

Objection 8. Paper trails meet objections 1-7 and make DREs minimally acceptable. As we have seen, this is not true. The paper trail does no more than persuade the voter that her vote was initially captured properly, but at the risk of announcing to the voter that the whole process is so insecure that her own vigilance is necessary. If the voter has to be watching at the polling place, what sort of confidence will she have in the remaining procedures that are conducted outside her presence? We have shown a number of alternatives to paper trails that genuinely meet the objections raised.

DRE machines have been described, somewhat dramatically, as a threat to democracy³⁹. A far greater threat to democracy is a return to any form of paper ballot, but both of these pale in comparison to the fact, not widely known, that in each presidential election more than 5 million Americans who are eligible to vote and want to vote are unable to cast a ballot because they happen to be outside their home districts on election day and cannot comply with their state's absentee procedures. Many of these people are overseas. The claim that tens of thousands of Floridians were disenfranchised in the 2000 election because of butterfly ballots, though probably true, is insignificant when measured against the millions who were unable to obtain any ballot at all. If computer scientists are truly concerned about threats to democracy, that's one they should work on.

¹ The author is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University and an attorney admitted to practice in the Commonwealth of Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 he was statutory examiner of electronic voting systems for the Commonwealth of Pennsylvania. From 1987-2000 he was the designee of the Attorney General of Texas for voting system certification. During those years he personally examined more than 100 different computerized voting systems for certification purposes. In the 2000 election, machines for which he participated in certification (which did not include Florida) were used to count more than 11% of the popular vote of the United States. This paper was prepared to accompany the author's appearance on an electronic voting panel at the ACM Computers, Freedom & Privacy Conference held in Berkeley, California in April 2004.

² The feminine pronoun is used to drive home the fact that a majority of U.S. voters are women.

³ Shamos, Michael, "Computerized Voting – Evaluating the Threat." Proc. Third ACM Conf. on Computers, Freedom & Privacy. San Francisco, CA (Mar. 1993). Available at <http://www.cpsr.org/conferences/cfp93/shamos.html>.

⁴ National Transportation Safety Board Publication NTSB/SR-02/02, "Safety Report: Transportation Safety Databases," September 11, 2002. Available at <http://www.nts.gov>.

⁵ Leveson, Nancy et al., "An Investigation of the Therac-25 Accidents," *IEEE Computer* 26, 7, pp. 18-41 (July 1993).

⁶ Available from the Federal Election Commission website at <http://www.fec.gov/pages/vssfinal/vss.html>.

⁷ N.Mex. Stat. Ann. 1-20-5 provides, "Unlawful opening of a voting machine consists of, without lawful authority, opening, unlocking, inspecting, tampering, resetting or adjusting a voting machine owned by any county, or conspiring with others to have the same done. Whoever commits unlawful opening of a voting machine is guilty of a fourth degree felony." In general, tampering is a felony but the penalties are probably not sufficiently high.

Quaere whether under the New Mexico statute a manufacturer who ships rigged software would in fact be committing this crime, which seems to require modification of a machine after it has become owned by a county.

⁸ U.S. Bureau of the Census, "Population Estimates for the 100 Largest U.S. Counties: April 1, 2000 to July 1, 2002," available at <http://eire.census.gov/popest/data/counties/tables/CO-EST2002/CO-EST2002-09.php>. Six of the 35 counties are in New York; another six are in California.

⁹ Thompson, Ken, "Reflections on Trusting Trust," *CACM* 27, 8 pp. 761-763, August 1984.

¹⁰ Neumann, Peter, "Risks in Computerized Elections," *Inside Risks* 5, *CACM* 33, 11, p.170, November 1990

¹¹ Jefferson, David et al., "A Security Analysis of the Secure Electronic Voting and Registration System (SERVE)," Jan. 21, 2004. Available at <http://www.servesecurityreport.org/paper.pdf>.

¹² Available from the Federal Election Commission website at <http://www.fec.gov/pages/vssfinal/vss.html>.

¹³ There is one reference in HAVA to the FEC Standards, but it pertains to acceptable error rates in ballot counting. 42 U.S.C. §15481(a)(5).

¹⁴ 42 U.S.C. §15481(a).

¹⁵ Article I, Sec. 4 of the U.S. Constitution provides: "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of choosing Senators."

¹⁶ Bannet, John, "Hack-a-Vote: Security Issues with Electronic Voting Systems," *IEEE Security and Privacy Magazine*, Jan/Feb 2004.

¹⁷ Bill S. 1986, 108th Congress, First Session.

¹⁸ 12 C.F.R. §205.9.

¹⁹ 12 C.F.R. §205.17.

²⁰ 12 C.F.R. §205.17.

²¹ There is a type of document of title known as a "warehouse receipt," which is necessary for a buyer to secure possession of his goods in certain situations, that has special status under the Uniform Commercial Code. But this is not the sort of receipt one ordinarily receives from a merchant in a sale transaction.

²² New Hampshire Lottery Rule 7(C).

²³ The largest U.S. lottery payout in history, \$363 million, resulted from the May 9, 2000 drawing in The Big Game, a multistate lottery now known as "Mega Millions."

²⁴ In his CFP '93 paper the author endorsed the use of state lottery systems for voting (without giving receipts, of course) and still does because their security and reliability is proven daily all around the country and they are clearly trusted by the public.

²⁵ 15 U.S.C. §7001 ff.

²⁶ 15 U.S.C. §7001(a)(1).

²⁷ The Food and Drug Administration regulations are typical: "Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper." 21 C.F.R. §11.1(c).

²⁸ UETA Comment 1(f).

²⁹ F.R.E. 1001 reads, "For purposes of this article the following definitions are applicable: (1) Writings and recordings. 'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."

³⁰ Press release of the Indiana Business Modernization and Technology Corporation, Dec. 21, 2001.

³¹ Fla. Stat. §102.061.

³² Mira, Leslie, "For Brazil Voters, Machines Rule," *Wired News*, Jan. 24, 2004.

³³ Standard 2.1.1.4, "State of California DRAFT STANDARDS For Use of Accessible Voter Verified Paper Audit Trail Systems in Direct Recording Electronic (DRE) Voting Machines," Secretary of State of California, March 18, 2004.

³⁴ Selker, Ted. et al, "The SAVE System: Secure Architecture for Voting Electronically: Existing Technology, with Built-in Redundancy, Enables Reliability," CalTech/MIT Voting Project VTR Working Paper, Oct. 22, 2003, revised January 4, 2004.

³⁵ It is actually not difficult to deduce this information from the ballot programming, which usually contains the date of the election in a predefined text field, the presence of which could be required by the system.

³⁶ See note 16. Hack-a-Vote is a project in which students are asked to develop malicious vote-counting software and other students try to find the malicious portions. It's not easy when posed in that framework.

³⁷ According to the Bureau of Labor Statistics, in 1990 there were about 881,000 computer scientists and mathematicians in the U.S.

³⁸ Spannaus, Edward, "Electronic Voting is Threat to the Constitution," *Executive Intelligence Review*, Jan. 30, 2004.

³⁹ Zetter, Kim, "How E-Voting Threatens Democracy." Wired.com, Jan, 29, 2004.