INTRODUCTION

This lawsuit is brought to ensure that every vote cast in New Jersey in the upcoming November 2004 general election is counted. The right to vote is fundamental. It is one of the most highly protected rights in New Jersey. Courts in this State have consistently made clear that the intent of the voter must be tabulated, and that every step of the election process must be fair and transparent. Electronic voting machines, otherwise known as Direct Recording Electronic voting machines ("DREs"), are scheduled to be used in fifteen of New Jersey's twenty-one counties.[1] Those machines cannot be relied upon to protect the fundamental right to vote in any circumstance, but particularly in the upcoming election.

Recent polls, including those by the New York Times/CBS News, Gallup International, the Rasmussen Report, and NBC news show that the two major presidential candidates, President George W. Bush

---

[1] The inventory list posted by the Attorney General erroneously stated that 16 NJ counties use DREs. The report erroneously states that Warren County uses DREs. This information is incorrect. Warren County voters vote using Op-Tech III-P Eagle optically scanned paper ballots. Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004, at http://www.njelections.org/voting_machine_co_list_doe.html (last visited Oct. 15, 2004).

(R), and Senator John Kerry (D) are consistently polling within ten points of each other, making the race neck-and-neck.[2] Polls have also indicated that in New Jersey, the contested race may be even closer.[3] Given that New Jersey is a "swing state," preserving the accuracy of the vote count and the intent of the voters is paramount.

Many reputable studies written by computer scientists (discussed in detail herein) have shown that DREs are unreliable and prone to errors. Machine models scheduled to be used this

---

2 Polls are recent as of October 18, 2004. The New York Times/CBS News Poll, September 12-16, 2004, available at http://www.nytimes.com/ref/politics/WEB-POLLINDEX.html (Sept. 19, 2004); Gallup National Snapshot, available at http://www.gallup.com/election2004/showdown/; Rasmussen Reports Presidential Tracking Poll, available at http://www.rasmussenreports.com/Presidential_Tracking_Poll.htm (last modified Oct. 18, 2004); MSNBC Election Scorecard, available at http://www.msnbc.msn.com/id/6028629 (last modified Oct. 18, 2004).

3 Polls are recent as of October 18, 2004. The New York Times/CBS News Poll, September 12-16, 2004, available at http://www.nytimes.com/ref/politics/WEB-POLLINDEX.html (Sept. 19, 2004); Gallup National Snapshot, available at http://www.gallup.com/election2004/showdown/; Rasmussen Reports Presidential Tracking Poll, available at http://www.rasmussenreports.com/Presidential_Tracking_Poll.htm (last modified Oct. 18, 2004); MSNBC Horserace Election Scorecard, available at http://www.msnbc.msn.com/id/6028629 (last modified Oct. 18, 2004).

Election Day have been unable to transmit voting totals,[4] had technical malfunctions during elections,[5] and registered votes for the wrong candidate.[6]

Computer scientists, who are uniquely qualified to assess DRE technology (and who are not normally associated with political activism), have become very vocal in opposing unsecure DREs. They have encouraged elected and other governmental officials to enact legislation implementing stringent security measures for DREs, including requiring that a verifiable paper ballot be a required component of DREs.

Indeed, the October 2004 issue of the prestigious periodical Communications of the ACM ("CACM") was almost entirely devoted to discussing the problems with electronic voting. Communications of the ACM, Oct. 2004. One study in the edition, conducted by a team of Yale University researchers, concluded that the manipulation of simply one vote per machine would have been enough to change the

---

4Jeff Testerman, Officials Still Searching for Election Glitch: The New Systems Could Not Send the Tabulations to the Elections Office, St. Petersburg Times, Apr. 6, 2002, at 3B.

5Wyatt Olson, Out of Touch: You Press the Screen. The Machine Tells You Your Vote has Been Counted. But How Can You be Sure?, New Times Broward Palm-Beach, available at http://www.newtimesbpb.com/issues2003-04-24/feature.html/1/index.html (Apr. 24, 2003).

outcome of the 2000 presidential election. Anthony DiFranco et al., Small Vote Manipulations Can Swing Election, Communications of the ACM, Oct. 2004, at 43, 44-45.

> Such slight manipulations, despite significantly changing the outcome of the election, are small enough that they might plausibly evade detection entirely, be dismissed as random noise if detected, be obscured by noise inherent in the voting and auditing process, or fail to prompt a recount if they are detected but their significance is underscored or misunderstood.

Id.

As of June 8, 2004, there were approximately 4.6 million registered voters in the state of New Jersey.[7] That number most certainly has grown in the recent weeks. See, e.g., Richard Cowen & Yung Kim, Voter Registration Crush in N.J.; Many Beat Deadline, Citing Presidential Race, The Record, Oct. 5, 2004, at A01; Rudy Larini, Signing to Vote in Nick of Time - N.J. Sees Landslide of Last-Day Registrations, Newark Star-Ledger, Oct. 5, 2004, at 1; Kate Zernike & Ford Fessenden, As Deadlines Hit, Rolls of Voters

---

6 Id.http://library.ardemgaz.com

[7] Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, Registered Voters as of the Close of Registration for the Primary Election to be Held on June 8, at http://www.state.nj.us/lps/elections/6-04-by-county.pdf(last visited Oct. 10, 2004).

Show Big Surge, N.Y. Times, Oct. 4, 2004, at 1. Of those, at least 3.3 million voters will be using DREs in November.[8]

Both Governor McGreevey and Attorney General Harvey have failed to respond adequately to Plaintiffs' and other New Jersey voters' growing concerns about the insecurity of DREs to accurately record their votes. Given the close nature of this year's Presidential race, it is essential that this Court intervene in order to preserve the integrity of the vote.

This Court should enjoin the use of DREs and order that all votes be cast on emergency paper ballots or absentee ballots that can be optically scanned by technology already possessed by most counties in the State. The Court should further order that all DRE machines be retrofitted with a voter verified paper ballot component before they can be used in any future election. Finally, this Court should order that all DREs purchased by any New Jersey counties in the future contain a voter verified paper ballot component.

This Court should issue the requested relief to ensure that the actual person chosen by the New Jersey electorate receives New Jersey's coveted 15 electoral votes.

---

[8] Id.; Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004.

FACTS

After the Florida debacle of the 2000 general election, the U.S. Congress enacted the Help America Vote Act of 2002 ("HAVA"), which became law on October 29, 2002, to "ensure that every eligible voter has the opportunity to vote, that every vote will be counted that should be counted, and that no legal vote will be cancelled by a fraudulent vote." N.J.S.A. § 19:61-1(b(2004)). This legislation provided $3.8 billion to improve the election process; $325 million of this sum was specifically allocated to states to update their voting systems. Help America Vote Act of 2002, 107 P.L. 252 §101, 116 Stat. 1666, 1668-70 (2002).

Many states took this opportunity to purchase DREs. These actions proved to be hasty. Sufficient research was not conducted prior to purchasing the DREs regarding the deficiencies of the systems. Moreover, state election laws were not updated to regulate the use of DREs.

DREs will be used in fifteen New Jersey counties in the upcoming November 2004 election. NJ Voting Equipment Inventory as of March 2004. Below is a list of voting machines each county

intends to use on Election Day, and the number of registered voters in each county as of June 8, 2004:

> Atlantic County: 230 Shoup Shouptronic 1242 electronic machines. Atlantic County has 141,895 registered voters.
>
> Bergen County: 1,200 Sequoia Pacific[9] AVC Advantage machines. Bergen County has 487,219 registered voters.
>
> Burlington County: 500 Sequoia Pacific AVC Advantage machines. Burlington County has 242,701 registered voters.
>
> Gloucester County: 520 Sequoia Pacific AVC Advantage machines. Gloucester County has 160,083 registered voters.
>
> Hudson County: 600 Sequoia Pacific AVC Advantage machines. Hudson County has 276,205 registered voters.
>
> Hunterdon County: 127 Sequoia Pacific AVC Advantage machines. Hunterdon County has 74,841 registered voters.
>
> Mercer County: 600 Sequoia Pacific AVC Advantage machines. Mercer County has 189,717 registered voters.
>
> Middlesex County: 662 Sequoia Pacific AVC Advantage machines. Middlesex County has 391,106 registered voters.
>
> Morris County: 805 Sequoia Pacific AVC Advantage machines. Morris County has 290,659 registered voters.
>
> Ocean County: 704 Sequoia Pacific AVC Advantage machines. Ocean County has 330,229 registered voters.

---

[9] Sequoia Pacific AVC Advantage and Sequoia Pacific AVC Edge machines are manufactured by Sequoia Voting Systems, which changed its name from Sequoia Pacific. See Steve Ellman, Contract Law, Miami Daily Business Review, Sept. 30, 2003, at 1.

Passaic County: 420 ES&S V-2000 machines. Passaic County has 234,017 registered voters.

Salem County: 160 Sequoia Pacific AVC Edge machines. Salem County has 40,245 registered voters.
Somerset County: 290 Sequoia Pacific AVC Advantage machines. Somerset County has 154,856 registered voters.

Sussex County: 361 ES&S iVotronic machines. Sussex County has 82,624 registered voters.

Union County: 500 Sequoia Pacific AVC Advantage

machines. Union County has 263,068 registered voters.

None of these DREs are equipped with voter verified paper ballots. Thus, votes can be erased by the machines and never be detected. Certification of Andrew Appel 14-15 (Oct. 14, 2004); Certification of Rebecca Mercuri Certif. 38-47 (Oct. 17, 2004).

Alarmingly, the process for certifying voting machines in New Jersey is grossly outmoded and cannot be applied readily to DREs. Thus, there is no way to determine whether the software in DREs is functioning properly, or if it has been corrupted to manipulate election results.

Plaintiffs, Assemblyman Reed Gusciora, New Jersey Peace Action, and Coalition for Peace, have tried to work with Governor McGreevey and Attorney General Harvey since the spring of 2004 to try to make DREs more secure. They have been stonewalled.

Plaintiff Stephanie Harris attempted to cast her vote four times during the June 2004 primary election in Mercer County. She has no way of knowing whether her vote was cast at all. Certif. of Stephanie Harris, Oct. 13, 2004, 8.

Plaintiffs implore this Court to step in where the Governor and Attorney General have failed to take action. This Court is tasked with upholding the statutory and constitutional laws of this State, regardless of the actions of elected and appointed governmental officials. This Court should grant Plaintiffs' requested relief to preserve the fundamental right to vote.

II. VOTING BY DRE IS AN INHERENTLY INSECURE PROCESS.

Electronic balloting and tabulation systems are inherently insecure and unreliable. Unless votes can be independently audited, there is no way to ensure that what a voter sees on a DRE screen is accurately recorded in the counting device. Appel Certif. 10-12; Mercuri Certif. 9, 38-47; Summary a-g.

A. It Is Impossible To Determine Whether DRE Software Is Actually Executing the Program It Is Supposed To Be Executing.

DRE ballots are laid out so that, at least visually, there is a logical connection between the candidate's name and the

button/touch screen that the voter presses to cast her ballot. Appel Certif. 10. This layout can lull the voter into a false sense of security. The visual logic of the ballot layout is misleading. Indeed, there is no connection (in either the hardware or software of a DRE) between the candidate's name, and the button/touch screen next to the candidate's name. Id. at 10-11. "Because there is no inherent internal connection between the buttons, the indicators, and the totals kept in memory, faulty software could very easily add a number to the wrong total when a button is pressed, or make some other error, thereby misrecording a vote." Id. at 11. Recording the voter's intent is entirely up to the discretion of the software. Id. at 13. It is critical then that software in DREs be reliable and trustworthy. Id. Placing unwavering faith in DRE software cannot be justified in light of the overwhelming evidence of DREs' insecurity.

It is a tenet of computer science theory that it is impossible to know for certain that any computer is performing a certain set of tasks, and no more. Mercuri Certif. 9. Indeed, it is impossible to prove that any computer is not infected with malicious code. Id. This also holds true for DREs. "The impact of this fundamental flaw on voting systems means that no matter

how stringent the testing and certification may be, this can not guarantee that the system will be 100% secure and 100% reliable." Id.

If the DRE software were made available for public inspection, trusting it (in the manner of the Attorney General and the Governor) might be somewhat more understandable. But, the software is not published. DRE manufacturers consider it a "trade secret," and guard it vigorously. Mercuri Certif. ¶¶ 7, 12, 26-27.

The only DRE software that has ever been published (that of the Diebold AccuVote, Appel Certif. ¶ 24) was found by computer security experts to be so seriously flawed that several states de-commissioned the use of all DREs until stringent security measures were implemented. Given the fundamental nature of the right to vote, we must assume, unless presented with proof to the contrary, that DREs are insecure. We must then act accordingly, to ensure that the fundamental right to vote is protected.

Unfortunately, current methods of testing are inadequate to discover malicious software. Most testing performed on DREs is called "black box" testing. Black box testing includes all kinds of testing that is done without knowledge of the internal workings

of the computer. Appel Certif. 18. Black box testing is performed out of necessity because DRE manufacturers will not permit their software to be inspected. Poll workers conduct black box testing before elections to see if the DREs work. They cast a certain number of ballots for each candidate, printing the totals, and verifying the machine tabulated the totals correctly. Id. Black box testing is useful in catching only some kinds of programming mistakes. Id.

However, black box testing is insufficient to discover fraudulent software. Id. at 19. Computers, including DREs "know" the time and day. Id. Thus, DREs can be programmed to perform according to expectations during pre-election tests, and then to activate a malicious code on Election Day that will sabotage the election. Id.

It is not difficult to write a computer program that can sabotage an election, and then cover its tracks. Indeed, any individual with basic knowledge of computer programming can write code that would cause a computer to display "A" on the screen, record "B" in its hardware, and "lie" to the tester by stating that it recorded "A" (when it had in fact recorded "B"). Mercuri Certif. 38; see also Appel Certif. 27.

> If a program is stored on a medium that is writable, such as an ordinary hard disk or a RAM memory cartridge, then it can modify itself. This means that a fraudulent program can be programmed to throw an election, and then at 7:55 p.m. on election day, overwrite itself with a copy of the certified, nonfraudulent program. This property of software-the inherent erasability [sic] of the medium-is unlike mechanical machines or paper.

Appel Certif. 31.

Programming errors are very difficult to detect, even among experts. Microsoft's products illustrate this point. Even though Microsoft has great financial incentive to produce completely foolproof programs, and hires testers and inspectors to insure that it produces the best product possible, program bugs still slip through and are passed on to the public. Id. at 25. This shows two things. One, that even well-trained, well-paid, and highly-motivated computer scientists who are looking for "bugs" cannot produce 100% accurate programs; and two, that unintentional "bugs" are very hard to detect. Id. at 25-26.

If unintentional bugs are difficult to detect, malicious bugs implanted in software, that are deliberately hidden, are even more difficult, if not impossible to detect. Id. at 27. Such fraudulent software is easy to install in DREs.

Fraudulent election software can be installed in DREs during the manufacturing stage, or after their manufacture. Appel

Certif. 54. Every time a program is updated, the software can be corrupted. Id. at 60.

> Even the smallest change to a computer program-even a change of just one letter-can radically alter its behavior. It is entirely possible that program bugs (which could miscount the vote) or fraudulent modification s to the program could be inserted into "upgrades". Therefore it is absolutely necessary that, if the manufacturer makes changes tot he software, the new version fo the software is subjected to . . .[a] scrupulous certification process. . .

Id. at 60. Moreover, election software can be corrupted whenever the software is used in conjunction with a commercial software or ancillary computer equipment. Mercuri Certif. 49.

Because the DREs are physically insecure, software can also be corrupted when DREs are left unattended for as little as five minutes, in some cases. Appel Certif. ¶ 50. Thus, a DRE's software can easily be overridden and corrupted while the machine is being transported, stored, or even under the noses of inattentive poll workers on Election Day.

Because fraudulent software is so difficult to detect, the public, including computer security experts, have no way of knowing whether DRE software is tainted. DRE manufacturers guard their software vigorously, arguing that it is protected by trade secrets. Mercuri Certif. 7, 12, 26-27. The public cannot

trust that voting software is not tainted, particularly because there have been so many instances where DREs have lost votes. Moreover, manufacturers have not been forthcoming in acknowledging problems with their products. For example, ES&S, which sold 361 iVotronic machines to Sussex County, supplied machines with uncertified software to several states. Id. at 22, 48-54.

B. The Only Way To Ensure the DREs Are Functioning Properly, Is To Conduct An Independent Audit, Using Voter Verified Paper Ballots.

The only way to ensure that DREs are not manipulating our votes is to conduct an independent audit of election results. To ensure that every vote is counted, every voter using an electronic voting machine must be able to personally check whether the DRE has accurately recorded his/her vote. The most reliable method for doing so is through the use of a "voter verified ballot system"[10] which is also called the "Mercuri Method." The Mercuri Method was devised by Rebecca Mercuri, Ph.D, Plaintiffs' expert.

[10] "Note that a 'voter verified paper ballot' (VVPB) or 'voter verified paper audit trail' (VVPAT) is NOT the same as a 'voter verifiable audit trail' (VVAT). . . ." Mercuri, Electronic Voting:

Who Created the Voter Verified Balloting Concept?, available at http://www.notablesoftware.com/evote.html (last modified Mar. 6, 2004).

> Mercuri Method - a paper ballot is prepared using an electronic voting system and displayed behind a transparent window. The voter is provided with an opportunity to verify the choices printed on the paper ballot prior to performing an action that deposits the ballot into a secured ballot box. The voter must also be provided with a way of voiding the ballot prior to casting if it is incorrect and, in such a case, must be provided with another opportunity to verify and cast a ballot.

Mercuri Certif. ¶ 42.

> Simply adding paper "receipts" to [a voting] system is not sufficient. The voter must be required to perform an action that confirms that their choices have been recorded correctly on the paper, hence making it a verified (rather than just "verifiable") ballot in a legal sense. The paper ballot must not provide any feature that could be used to violate voter privacy or encourage coercion and vote selling. These voter verified paper ballots should be used to produce the certified vote totals and be available for scrutiny in

> case of election contest or recount. When properly implemented, the "Mercuri Method" ensures that paper ballots will not be removed from the polling place nor added to the ballot box.

Mercuri, Electronic Voting. By using the Mercuri Method, it would be possible to determine if the vote cast by the voter is, in fact, the vote recorded by the machine. Such a verification would assuage any reservations that a voter might have about using DREs. Rebecca Mercuri, Humanizing Voting Interfaces.[11]

The use of voter verified paper ballots, as an effective means of independently auditing votes, has been endorsed by voting technology research studies conducted across the country. RABA Technologies, LLC., Trusted Agent Report: Diebold AccuVote-TS Voting Systems 8, 23 (2004); Aviel Rubin et al., Analysis of an Electroniv Voting System 21 (2004); Science Applications International Corporation ("SAIC"), Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes 5 (2003).

III. RESEARCH STUDIES SHOW THAT DRE VOTING MACHINES, INCLUDING THE MODELS SCHEDULED TO BE USED IN NEW JERSEY, HAVE MANY SECURITY VULNERABILITIES.

[11] At http://notablesoftware.com/Papers/UPAPaper.html (July 11, 2002).

A handful of the many studies criticizing the security vulnerabilities of DRES are summarized below. They were chosen to illustrate how the insecurity of DRE voting system software and hardware presents far too many opportunities for tampering with election results.

A. A CalTech/MIT Voting Study Showed That DREs Are Less Reliable Than Paper Ballots.

In July 2001 The CalTech/MIT Voting Technology Project released the results of a study entitled Voting: What Is, What Could Be,[12] comparing the performance of paper ballots, punch cards, lever machines, optical scan machines, DREs, and machines using mixed technologies. The study found that DREs were more unreliable than paper ballots. Id. at 24.

The study examined the reliability of these different machines by comparing the residual vote rates between the 1988 and 2000 elections. Residual votes rates are those votes entered into a voting machine which for various reasons are not included or tabulated into final election results. Id. at 22.

Residual votes are a measure of reliability because residual votes in elections vary depending upon the type of voting

[12] Available at http://www.vote.caltech.edu/Reports/july01/July01_VTP_%20Voting_Report_Entire.pdf (last visited Oct. 15, 2004).

equipment used. Id. at 22-24. Thus, the ability of voters to express their preferences in an election is related to the type of voting machines used.

The CalTech/MIT Study found that paper ballots are most reliable and have the lowest average median residual vote rates, preserving voter preferences more frequently than other voting technologies. Id. at 23. The study showed that the residual vote rate of punch card methods and electronic devices were 50% higher than the residual voting rate of manually counted paper ballots. Id. at 21,[13] 24. The report discouraged the use of newly developed touchscreen electronic voting machines because they are "still unproven." Id. at 22.

---

[13] The CalTech/MIT Voting Technology Project has found that electronic voting machines have produced high residual vote rates in all elections since the study began in 1998, except during the year 2000. During the year 2000 punch card systems had higher rates of uncounted votes than other available technologies. Id. at 6. This undoubtedly contributed to the 2000 Florida election debacle.

In addition, a study conducted this year by the Florida Sun Sentinel found that DREs have a residual vote rate six times greater than optically scanned ballots. Mercuri Certif. 15. "In close elections, these 'missing' votes can certainly affect the outcome of a race [even] if they were not intentional." Id.

B. Three Research Studies Examining DRES Conducted By The State Of Maryland Showed That DRES Were Unreliable And Insecure.

During a September 2002 primary election, voters in the State of Maryland experienced serious problems while using thousands of touchscreen electronic voting systems. These machines were manufactured by the Diebold Corporation.

In early February 2003, journalist Bev Harris reported that by performing a simple "Google" search she had visited a file server used by Diebold's programmers, and was able to exchange and update parts of Diebold's allegedly secure software. The server contained all of the tools necessary to manipulate the Diebold software and machines. It contained passwords/encryption keys, source code, user manuals, testing protocols, and files containing voting records and voting machine software. Bev Harris, Voting System Integrity Flaw Discovered at Diebold Election Systems, Scoop, Feb. 5, 2003 and Feb. 10, 2003.[14] The accessibility of this

[14] Available at

server was, itself, a major security vulnerability because it allowed access to programming information which made a host of voting machine manipulations possible.

Following the publication of Ms. Harris's findings, a series of research studies conducted during 2003 and 2004 revealed very serious security vulnerabilities in the software, source code, encryption and passwords used by the Diebold DRES.

A team of computer science experts from Johns Hopkins University Information Security Institute and Rice University investigated the Diebold source code discovered by Bev Harris. They published a technical report, known as the "Hopkins Report."[15] The Hopkins Report outlined in detail security vulnerabilities of the voting system's software, and other system components. Most importantly, the Hopkins Report showed that attacks on election results could be made even without access to the softwar that is

---

http://www.scoop.co.nz/mason/stories/HL0302/S00052.htm.

15 This report was first published by the IEEE Computer Society Press in the IEEE Symposium on Security and Privacy 2004 as the Johns Hopkins University Information Security Institute Technical Report TR-2003-29 in July 23, 2003. The Report was authored by authored by Tadayoski Kohno, Adam Stubblefield, Aviel Rubin, and Dan S. Wallach. It was later republished on February 27, 2004 as Analysis of an Electronic Voting System. It is commonly referred to as the Hopkins Report in research and articles.

considered the "brain" of the computer. Rubin at 1; see Mercuri Certif. Exhibit B.

Following the release of the Hopkins Report, the State of Maryland commissioned an investigation of the security of Diebold's electronic voting machines. The Science Application International Corporation ("SAIC") conducted one investigation and released a Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes ("SAIC Report") on September 2, 2003. On November 10, 2003 the State of Maryland commissioned a second report by RABA Technologies, LLC. ("RABA"), an organization comprised of computer programming experts (that did not profit from their recommendations). Their report, Trusted Agent Report: Diebold AccuVote-TS Voting Systems ("RABA Report"), was published on January 20, 2004.

The three Maryland reports describe in detail the many security vulnerabilities of the DREs that had been used in the Maryand primary (including multiple ways the machines could be hacked without detection, leaving votes open to manipulation at every step of the voting process). The alarming findings of the Maryland reports will not be summarized herein because they deal only with DREs manufactured by the Diebold Corporation,

particularly the Deibold AccuVote-TS voting systems; none of which are scheduled to be used in New Jersey.

The significance of the Maryland reports is that they were written by computer security experts who had a comprehensive understanding of the hardware and software of the Diebold machines. Those scientists had access to Diebold software. This was unusual, as DRE manufacturers vigorously protect their software, asserting that they are trade secrets. Mercuri Certif. 7, 12, 26-27.

The Maryland reports were a wake-up call to all voters and election officials who believed that new technology would solve the many problems associated with running elections. The reports sparked a national examination of DREs. Many states subsequently conducted their own studies to determine whether DREs they had already purchased could be trusted to record votes accurately. Notably, those states that conducted their own studies of DREs concluded that the models they inspected had serious security flaws and could not be relied upon to count votes. These flaws existed, even though the DREs had received formal certification. Appel Certif. ¶ 64; Mercuri Certif. ¶¶ 22, 34, 41. As a results, many states have implemented stringent security requirements. The

Defendants have chosen to ignore, rather than embrace this scrutiny of DREs.

C. A Study Commissioned By the State of Ohio Revealed That DRE Voting Systems Identical To Those Scheduled To Be Used In New Jersey Have Serious Security Flaws.

Secretary of State J. Kenneth Blackwell contracted with two technology security review firms to assess the safety and reliability of certain models of DREs. J. Kenneth Blackwell, The Process of Implementing HAVA is Critical to Success, The Spirit of Citizenship & Democracy, Winter 2004, at 3.[16] The firms were the Compuware Corporation, a for-profit information technology firm, and InfoSENTRY, Services, Inc., a for-profit computer consulting firm.

Four vendors' systems were reviewed by the two firms: Election Systems & Software (ES&S), Diebold Electronic Systems, Maximus/Hart Intervivic/DFM Associated, and Sequoia Voting Systems. Tom Chansky, Comprehensive Study Charts Path to Success, The Spirit of Citizenship & Democracy, Winter 2004, at 4.[17] None

---

16 Available at http://www.sos.state.oh.us/sos/http://www.sos.state.oh.us/sos/pubAffairs/ spirit/winter2004.pdf (last visited Oct. 12, 2004).

17Available at http://www.sos.state.oh.us/sos/pubAffairs/spirit/winter2004.pdf. (last visited Oct. 10, 2004).

of the four vendors' systems passed either security review. Id. Two of the failed systems are scheduled to be used in New Jersey in November 2004: ES&S's iVotronic and Sequoia Voting Systems' AVC Edge.[18]

1. Both Security Firms Retained By Ohio Found Critical Problems With The ES&S iVotronic.

Compuware found 17 total problems with the ES&S iVotronic, Stephen Mayo, PMP, Ohio Sec'y of State DRE Technical Sec. Assessment, 13 (Dec. 2, 2003)[19], three of which were labeled critical. Compuware Corporation, Direct Recording Electronic (DRE) Technical Security Assessment Report, 141 (Nov. 21, 2003).[20] The first of these was that ES&S "does not use encryption to protect election data transferred to and from the iVotronic. There is a risk that an unauthorized person could gain access to

---

18 Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004, at http://www.njelections.org/voting_machine_co_list_doe.html.

19 Available at http://www.sos.state.oh.us/sos/hava/files/compuwarepress.pdf (last visited Oct. 10, 2004).

20 Available at http://www.sos.state.oh.us/sos/hava/files/compuware.pdf (last visited Oct. 10, 2004).

election data." Id. Compuware recommended that ES&S "incorporate strong encryption to protect data." Id.

A second problem was that supervisory passwords installed by ES&S are not "hardcoded." Id. Therefore,

> [i]f an attacker with knowledge of these passwords can access a [cartridge used to activate voting machines] configured for the current election, they [sic] can execute supervisory functions including casting unauthorized votes and closing the polls early. There is a risk that an unauthorized person with knowledge of the supervisory passwords and access to a Supervisor PEB [which resets machines and activates ballots] could cast multiple ballots.[21] Id.

Compuware also found that the iVotronic's software was problematic. Id.

---

21 Compuware recommended "that ES&S incorporate user-changeable passwords of at least six characters in length. . . . [and] that administrative policies and procedures be put into place regarding password management and physical security of the Supervisor PEBs." Compuware at 141.

> [It] allows the user to perform an "ADD TO" function, which adds results from a DRE to a precinct's totals. This function does not detect when a DRE['s] [totals are] added more than once resulting in incorrect vote tallies. There is a risk that the election results for a DRE can be uploaded to the . . . software multiple times, and the votes would be counted multiple times.[22] Id.

---

22 Compuware's recommendation was a software modification by ES&S to "prevent duplicate counting of votes." Compuware at 141.

InfoSENTRY[23] found problems with the ES&S iVotronic, four of which have critical implications in New Jersey. "ES&S [did] not perform[ ] an internal, detailed security risk assessment" on its entire system; ES&S's minimal security audit focused on the company's financial systems and neglected its "information systems infrastructure and products;" ES&S provided insufficient training on information security for its administrators and staff; ES&S did not obtain industry quality certifications for its processes, facilities, and software. InfoSENTRY at 17-18.

2. Both Compuware And InfoSENTRY Found Significant Risks Present In Sequoia Voting Systems' AVC Edge Machine.

Compuware identified a total of 15 risks, Mayo at 13, seven of which were critical. Compuware at 250. Two of these risks involved the security of the memory card in the AVC Edge machine. Id. at 250-51. First, was the concern that "an unauthorized user could access unencrypted data stored" on the memory card. Id. at 250. Second, was the risk that the standard memory card used by Sequoia Voting Systems for "storing the ballot definitions and vote results . . ." could be corrupted in transit. Id. at 251.

---

23 The problems identified by InfoSENTRY are available at http://www.sos.state.oh.us/sos/hava/files/InfoSENTRY1.pdf (last visited Oct. 10, 2004).

The memory card "can be easily placed in a laptop and altered... [rendering it] unreadable by the DRE or election management software." Id.

Two risks involved the physical design of the Sequoia Pacific AVC Edge. Id. at 250-51. First, a button on the back of the machine could shift the machine into supervisor mode without a password. Id. at 250. Second, a switch on the back of the machine closed the polls. "No password is required to close the polls. . . . [and] an unauthorized person might close the polls on the AVC Edge." Id. at 251.

The final of three risks identified by Compuware all involved the lack of locking functions on the Sequoia Pacific AVC Edge. Id. at 250. No lock existed on the machine's voting booth case, resulting in "a risk that an unauthorized person could gain access to the AVC Edge during transportation to an election or while in storage." Id. A keyed seal protecting the power switch on the back of the AVC Edge was an optional feature. Its absence presented the risk that an unauthorized, or authorized, person could power off the machine during voting. Id.

A memory card could be removed if its compartment is not locked. Id. Manipulation of the memory card could cause the

DRE's entire software to be reprogrammed to tamper with voting. Id.

Compuware made recommendations to improve the security of the Sequoia Pacific AVC Edge. Compuware recommended Sequoia "incorporate strong encryption to protect data." Compuware, at 250. Compuware's recommended solution was very general: requiring "that administrative policies and procedures be put into place to mitigate this risk." Id. at 251. Compuware recommended "password protection for supervisor functions." Id. at 250. Compuware recommended that Sequoia Voting Systems install the optional keyed wire seal on these switches on all the machines, as well as "provid[ing] password protection for closing the polls." Id. at 251. Compuware also recommended the installation of seals and locks on all machines. Id. Compuware recommended the mandatory installation of these keyed switches on all machines' power switches. Id. Compuware also recommended the installation of locks on all machines. Id.

Among the risks discovered by InfoSENTRY in the AVC Edge were three with critical implications for New Jersey voters. First, Sequoia Voting Systems failed to have "an external network security assessment . . . [or] a detailed security risk

assessment" on its full system. InfoSENTRY at 21. Second, Sequoia Voting Systems failed to fully provide its information systems managers with security specific training. Id. Third, Sequoia Voting Systems failed to seek or attain industry standard certification. Id. at 22.

InfoSENTRY made recommendations to improve the security of the Sequoia Pacific AVC Edge, including immediately conducting a security risk assessment, and obtaining certification for the Sequoia Voting Systems machines. Id. at 21.

Secretary Blackwell endorsed the findings and recommendations of both Compuware and InfoSENTRY, stating that until each of the four vendors had corrected all identified problems, new machines would not be used in an election in Ohio. Chansky at 4. To date, none of the vendors have implemented the changes. Ohio will not permit the DREs it examined to be used in the upcoming election. Id. It will only permit the use of DREs that had been purchased and used before the study was conducted, and which have undergone adequate security checks to reduce risks. Id.

D. The Brennan Center for Justice And The Leadership Council On Civil Rights Poses A Security Risk.

Due to growing concerns over the vulnerability of DREs to security breaches and malfunction, the Brennan Center for Justice and the Leadership Conference on Civil Rights conducted an independent assessment of DRE system security during 2004.

The study sought to determine what security measures states should implement to ensure that all votes cast on DREs this November are counted accurately. The Brennan Center assembled a team of nationally renowned security experts including a former Cyber Security Advisor to the White House, a Certified Information Systems Security Professional with extensive experience engineering critical system, and a senior research scientist at Columbia University, to develop recommendations that would improve the security of DRES and voter confidence in these systems. The Brennan Center published Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems,("The Brennan Center for Justice Report")[24] in June 2004. "If implemented . . . within the obvious constraints of time and resources," the Report stated, "these recommendations can markedly

---

24 Available at http://www.brennancenter.org/programs/downloads/voting_systems_final_recommendations.pdf (last visited Oct. 15, 2004).

improve confidence that [DREs] will function properly on Election Day and that votes will be recorded and counted accurately." Id. at 2.

The report recommends that election officials hire a "well-qualified, independent security team" to conduct security risk assessments of DREs, including hardware/firmware design and configuration, DRE software design and configuration, election procedures and physical security. The report further recommends that election officials adopt any measures suggested by the security team, and thoroughly train officials in implementing these measures. Id. at 2-3.

The report also recommends that "red team" exercises, similar to those used by RABA Associates, be conducted on DRE software and hardware prior to the election. Id. at 6-7. To assure that software is secure, a "red team" should review source code and give special attention to authentication, encryption and the accessibility of voting records. Id. at 7. Experts should examine how data flows from one part of the computer to another to assess problems in software configuration. Id. Digital signatures should be placed on software to more easily distinguish malicious code. Id. at 8.

Security officials, the Brennan Center Report recommended, need to examine all locks and security devices on DREs. Id. at 9. They also need to examine the training of election officials. Id. Examiners must also look at the physical security of voting machines to be sure that they are kept out of reach of potential attackers while being stored, transported, and handled on election day. Id. at 10.

IV. ELECTRONIC VOTING MACHINES OF THE SAME MAKE AND MODEL AS NEW JERSEY DREs HAVE MALFUNCTIONED AND FAILED TO READ ACCURATELY VOTES CAST IN ELECTIONS THROUGHOUT THE UNITED STATES.

The expert reports and studies discussed above are not merely theoretical exercises conducted by academics. The malfunctions described by these computer science experts have all occured during elections.

Plaintiff Stephanie Harris believes she may have been disenfranchised by a Sequoia Voting Systems DRE in June 2004 in Mercer County. When she attempted to vote on a Sequoia Pacific AVC Advantage, the machine failed to register her vote three times. Certif. of Stephanie Harris, ¶¶ 3-7 (Oct. 1, 2004). She does not know, and has no way of knowing, whether her fourth attempt to vote was successful. Id. at 8. Eleven New Jersey

counties intend to use 6,508 AVC Advantage machines. NJ Voting Equipment Inventory as of March 2004.

In addition, Glenn Cantor had difficulty casting his ballot during a September 2004 election in Mercer County. When making his selection, a light appeared on the screen next to his choice, which very briefly went out before he could press the machine's "CAST VOTE" button. Certif. of Glenn Cantor, Oct. 17, 2004, 2. At that point, he could have left the polling site, but did not. On his own initiative, he consulted a poll worker, who told him to "'vote again.'" Id. at 5. The poll worker assured him he could vote repeatedly on a DRE, but that only one vote would be counted. Id. at 5. He attempted to do this repeatedly, and during one attempt, the DRE re-allocated his choice to a different selection. Id. at 8. After he pressed the "CAST VOTE" button three times, the poll worker realized she had failed to reset the DRE after the previous voter had cast his ballot. Id. at 9.

These examples of DRE malfunctions both occurred very recently in Mercer County. They demonstrate that DREs are not failsafe. They also demonstrate that it is difficult both for voters and poll workers to determine whether indeed votes have been cast. Ms. Harris and Mr. Cantor each pressed the "CAST VOTE"

buttons in the DREs they were using four times. This is highly problematic. Poll workers in Mercer County are advising voters to "vote again" when a DRE appears to not be functioning properly, rather than taking steps to determine whether the DRE should be de-commissioned.

As the following list of selected failures of Sequoia Voting Systems and ES&S electronic voting machines illustrates, it is quite possible that Ms. Harris and Mr. Cantor were indeed disenfranchised.

A. DREs Have Failed To Register Properly All Votes Cast.

1. Hillsborough County, FL (August 2004)

In a primary, 12,498 voters entered the voting booth but allegedly cast no vote for state attorney. Hillsborough County's undervote rate rose as high as 17% in that election. This rate was suspiciously high. Officials suspected votes were not registering properly on the DREs, but could not meaningfully re-examine the results because no paper audit trail existed. Jeff Testerman, Voting Mystery Stirs Call for Paper Trail, St. Petersburg Times, Oct. 4, 2004, at 1A. The

DREs were identified as Sequoia Pacific AVC Edge machines.[25] As previously stated, Salem County, which has over 40,000 registered voters, intends to use 160 of these machines.

2. Bexar County, TX (March 2004)

An ES&S iVotronic initially prevented a voter from casting his ballot for the candidate of his choice. He alerted poll workers, who cancelled his first vote and let him vote again. Tom Bower, Bexar Computer Glitch Delays Counting Of Votes, San Antonio Express-News, Mar. 10, 2004, at 12A. As previously stated, 361 of these machines are scheduled to be used in Sussex County.

3. Broward County, FL (January, 2004)

During a special election, the DREs failed to record 134 votes. Erika Bolstad, New System No Easy Touch For 134 Voters in Broward, Miami Herald, Jan. 8, 2004 at 1A. The machines were identified as ES&S iVotronics.[26] As previously

---

25 At http://www.votersunite.org/info/Sequoiainthenews.pdf (last visited Oct. 15, 2004).

26At http://www.votersunite.org/info/ES&Sinthenews.pdf (last visited Oct. 15, 2004).

stated, Sussex County, which has over 82,000 registered voters, intends to use 361 of these machines.

4. Miami-Dade County, FL (September 2002)

In 31 precincts, the votes of 8.2% of voters who signed in at the polls were lost. About half of the 1,544 lost votes were from African Americans. Problems causing the losses included the unavailability of working machines, as well as the failure of poorly trained poll workers to press the reset button on the machines. American Civil Liberties Union of Florida, Analysis of September 10th Voting Fiasco in Miami Dade Demonstrates Disproportionate Impact On Racial Minorities, ACLU Says.[27] These machines were identified as ES&S iVotronic machines.[28] As previously discussed, Sussex County has purchased 361 of these machines.

5. Palm Beach County, FL. (March 2002)

A candidate lost the election by four votes. The DREs failed to register seventy-eight votes. Additionally, the

---

27 At http://www.aclufl.org/news_events/archive/2002/racialimpactrelease.cfm (Oct. 21, 2002).

28 At http://www.votersunite.org/info/ES&Sinthenews.pdf.

machines acted erratically. Olson, Out Of Touch, New Times Broward-Palm Beach.[29] These machines were identified as Sequoia Pacific AVC Edge machines.[30] As previously stated, Salem County intends to use 160 of these machines.

6. Palm Beach County, Florida (March 2002)

---

29 Available at http://www.newtimesbpb.com/issues/2003-04-24/feature.html/1/index.html (Apr. 24, 2003).

30 Available at http://www.votersunite.org/info/Sequoiainthenews.pdf.

The favored candidate, who had enjoyed large leads in the polls, lost the election by a suspiciously large margin, losing even his home voting district. He contested the election, and sought to examine "inspection reports, testing protocols and codes on voting equipment." The county's attorney opposed the contest. The attorney argued that the top election official in the County would be committing a third-degree felony if she revealed the inner operations of the machine. The candidate's request was denied. (The contest suit was dismissed on other grounds.) Olson, Out Of Touch. These machines were identified as Sequoia Pacific AVC Edge machines.[31] As previously stated, Salem County intends to use 160 of these exact machines.

B. Flawed DRE Software Has Lost Votes.

1. Snohomish County, Washington (September 2004)

Software failed in 65 out of 860 machines, causing them to malfunction. In addition, there were problems with voter

---

31 Available at http://www.votersunite.org/info/sequoiainthenews.pdf.

"smart cards."[32] Paul Andrews, E-Voting Vent: You Can't Tell If It Worked, Seattle Times, Sept. 20, 2004, at E1.

2. State of Indiana (March 2004)

ES&S installed unauthorized and uncertified software in voting machines state-wide. Karen Hensel & Loni Smith McKown, Election Commission Bails Out Voting Machine Maker In Time For May Primary, Wish TV - Indianapolis, Mar. 11, 2004.[33]

C. DRE Cartridges Failed to Report Votes.

1. Morris County, NJ (June 2004)

The County's tabulation system could not read the DRE cartridges. The cartridges, rather than revealing election results, showed only zeroes. Election officials and computer experts worked through the night to correct the problem. Michael Daigle, County: No Problems With ID Checks, Daily Record (Morristown, NJ), June 10, 2004, at 12A. The machines were identified as Sequoia Pacific AVC Edge machines.[34] Salem

---

32 Smartcards are ATM-sized cards that activate some DREs.

33 At http://www.wishtv.com/Global/story.asp?S=1706282 (Mar. 11, 2004).

34 Available at http://www.votersunite.org/info/Sequoiainthenews.pdf.

County plans to use 160 of these machines, with the same counting cartridges.

2. Hillsborough County, FL (March 2003)

Precinct totals had to be manually entered after two data cartridges registered at the elections service center as "non-formatted." Because they were not formatted to store voting records, the cartridges were empty. Kathryn Wexler, Elections Chief Sees Nearly Flawless Vote, St. Petersburg Times, Mar. 5, 2003 at 3B. The machines were identified as the Sequoia Pacific AVC Edge.[35] As previously stated, Salem County intends to use 160 of these machines, with the same faulty cartridges.

3. Hillsborough County, FL (April 2002)

Precinct totals had to be manually entered after 24 out of 26 data cartridges malfunctioned and could not transmit vote totals. Jeff Testerman, Officials Still Searching for Election Glitch, St. Petersburg Times, Apr. 6, 2002, at 3B. These machines were identified as the Sequoia Pacific AVC

35 Available at http://www.votersunite.org/info/Sequoiainthenews.pdf.

Edge.[36] As previously stated, Salem County intends to use 160 of these exact machines, with the same faulty cartridges.

D. Vote Tabulation Systems Used With DREs Have Failed To Provide Accurate Vote Totals.

1. Natrona County, WY (August 2004)

Primary election totals in a number of municipal races had to be changed after vote-counting software malfunctioned. Matthew Van Dusen, Clerk Changes Election Vote Totals, Casper Star-Tribune.[37] Natrona County uses the ES&S Unity Election Management System.[38]

2. Miami-Dade County, FL (October 2003)

The audit log for DREs in Homestead, Florida completely failed to register the presence of five ES&S iVotronics. As a result, 162 votes were recorded on the vote image report but not in the audit log. Matthew Haggman, Another Vote Audit Flaw, Miami Daily Business Review, May 26, 2004, at 1. Sussex County intends to use 361 iVotronic machines.

---

36 Available at http://www.votersunite.org/info/sequoiainthenews.pdf.

37 Available at http://www.casperstartribune.net/articles/2004/08/21/news/casper/6c2e825b3f9e154187256ef70007adbb.txt (Aug. 21, 2004).

38 Available at http://www.votersunite.org/info/ES&Sinthenews.pdf.

3. Bernalillo County, NM (November 2002)

Software with a limited capacity to handle large amounts of data was overwhelmed by a ballot with more than 80 choices. Records showed that approximately 48,000 people voted at the early-voting sites, but initial vote totals showed no more than 36,000 votes for any candidate (including candidates for governor). Frank Zoretich, Election Results Certified After Software Blamed, Albuquerque Tribune, Nov. 19, 2002, at A2. These machines were identified as the Sequoia Pacific AVC Edge.[39] As previously stated, Salem County intends to use 160 of these machines.

4. Miami-Dade County, FL (April 2002)

Faulty programming caused a miscount of votes by listing candidate names in a different order on absentee ballots than on the touch-screen machines. The programming error led to incorrect vote totals, causing a losing candidate to be declared a winner and a winner to be declared a loser. Oscar Corral, Technician's Error, Not Machines, To Blame In Dade Election Mix-Up, Miami Herald Apr. 4, 2002 at 1A; Tech's Error Skews Florida Election Results, Deseret News (Salt Lake

39 Available at http://www.votersunite.org/info/Sequoiainthenews.pdf.

City) Apr. 4, 2002, at A07. These machines were identified as ES&S iVotronics.[40] As previously stated, 361 of these machines are scheduled to be used in Sussex County.

5. Riverside County, CA (November 2000)

A Sequoia Voting Systems tallying machine dropped votes from the tally. A Sequoia Voting Systems salesman reportedly intervened and "fixed" the problem. Elise Ackerman, Electronic Voting's Hidden Perils, San Jose Mercury News.[41] The voting system used Sequoia Pacific AVC Edge touch screens.[42] As previously stated, Salem County intends to use 160 of these machines.

E. Poorly Trained Poll Workers and DRE Industry Technicians Have Jeopardized Votes.

1. Riverside County, CA (October 2003)

Software used with the Sequoia Pacific AVC Edge touchscreen machines was left unguarded on a publicly-available server. The software controls how ballots are placed on the voting machines, and the counting and storing

---

40 Available at http://www.votersunite.org/info/ES&Sinthenews.pdf.

41 Available at http://www.independent-media.tv/item.cfm?fmedia_id=5450&fcategory_desc=Evoting%20Machines%20/%20vote%20Integrity (Feb. 1, 2004).

42At http://www.votersunite.org/info/sequoiainthenews.pdf (last accessed Oct. 10, 2004).

the votes after the election. Kim Zetter, E-Vote Software Leaked Online, Wired News.[43] As previously stated, Salem County intends to use 160 of these exact machines.

2. Palm Beach County, FL (March 2002).

Tabulation of election results was delayed when 15 data cartridges were lost because a poll worker "had taken them home." Olson, Out of Touch. The machines were identified as Sequoia Pacific AVC Edge.[44] Salem County has purchased 160 of these machines.

F. DRE Hardware Has Hampered Voting.

1. Santa Clara County, CA (March 2004)

Blind voters complained about malfunctioning audio features, braille on the machines that was installed upside-down, and instructions to press a yellow button (which are useless for blind voters). These mistakes seriously hampered blind voters' ability to vote. Elise Ackerman, Blind Voters Rip E-Machines: They Say Defects Thwart Goal Of Enfranchising Sight-Impaired, San Jose Mercury News.[45] These machines were

---

43 At http://www.wired.com/news/privacy/0,1848,61014,00.html (Oct. 29, 2003).

44 Available at http://www.votersunite.org/info/ES&Sinthenews.pdf.

45 Available at http://www.mercurynews.com/mld/mercurynews/news/breaking_news/8673336.htm?1c (May 15, 2004).

identified as Sequoia Pacific AVC Edge machines.[46] As previously stated, Salem County intends to use 160 of these exact machines.

G. The DREs Scheduled To Be Used In New Jersey Are Flawed And Cannot Be Relied Upon To Count Votes Accurately.

While the precise causes of most of the above-detailed DRE malfunctions are unknown, it is well known that the Sequoia Voting Systems and ES&S machines to be used in New Jersey are very insecure, and subject to manipulations, particularly by "insiders." Mercuri Certif. 18-22.

Anyone with physical access to a Sequoia Pacific AVC Edge machine for as little as five minutes, who knows the user password (which is not difficult to guess) can install a new program into the machine. Appel Certif. 50. That program can manipulate votes, and can throw an election without being detected. Id. at 12, 14.

New software that manipulates votes can also be installed in the AVC Edge by replacing a chip, which is protected only by a flimsy plastic seal, Id. at 51-53, 68, or by accessing a poorly protected port. Mercuri Certif. 20. If the chip is replaced, the new chip can re-program the

---

46 Available at http://www.votersunite.org/info/sequoiainthenews.pdf.

machine and can cause it to give votes to a particular candidate, regardless of each voter's choice. Id.

The Sequoia Pacific AVC Advantage has more "security features" than the Sequoia Pacific AVC Edge, but is still an insecure system. Appel Certif. 45. Like the Sequoia Pacific AVC Edge, the Sequoia Pacific AVC Advantage contains a cartridge with ballot information that can be easily reprogrammed using a key pad on the side of the machine. Mercuri Certif. 19, 28. Election workers, vendor staff, or anyone else with access to the DRE can change how the names of candidates are correlated with those printed on the paper that covers the button panel. Id. Thus, a vote cast for candidate "A" by the voter, will be attributed to candidate "B" by the manipulated DRE. Id.

The Sequoia Pacific AVC Advantage's software can also be reprogrammed by replacing its chip. This could be done by someone who has physical access to the machine for only ten minutes. Appel Certif. 51-53. Through the chip, the machine can be reprogrammed to give votes to whichever candidate the program on the chip tells it to, regardless of each voter's choice. Id. Reprogramming can cause the machine to manipulate votes, and to throw the election without being detected. Mercuri Certif. 20; see also Appel Certif. 12.

Moreover, there is a button on the back of a Sequoia Pacific AVC Edge and AVC Advantage that allows the machine to be locked after a vote is cast. Mercuri Certif. 23. This button sets the machine for the next voter. Id. Any poll worker can maliciously or inadvertently manipulate the election by depressing the exterior button several times and allowing a voter to vote more than once. Id. In the event of a recount, it would be impossible to distinguish these excess votes from other votes. Another button on the outside of the Sequoia Pacific AVC Edge is used to shut down the machine. Id. at 25. This relatively easy-to-access button invites tampering with the election.

Unauthorized users could easily access data and software stored on memory cartridges, including ballot definitions and voting results. Id. at 28, 50. The memory card on both the Sequoia Pacific AVC Advantage and AVC Edge is vulnerable to tampering via remote network connection. Appel Certif. 44.

Moreover, it is well-known that ES&S installed faulty and uncertified software in the DREs used in many states throughout the country and failed to recall the flawed software. Id. at 22. There is no way to be certain that the ES&S machines scheduled to be used in New Jersey are not tainted with the same faulty software.

ES&S iVotronic administrator passwords could be discovered very easily. Compuware Corporation, Direct Recording Electronic (DRE) Technical Security Assessment Report at 141. This discovery grants access to the ES&S iVotronic's software, and creates an opportunity to manipulate votes and cast multiple ballots without detection. Id. Moreover, ES&S iVotronic software permits the user to perform an "Add To" function, which adds results from a DRE to a precinct's totals. Id. This function does not detect when a DRE's totals are added more than once, resulting in incorrect tallies. Id. This "Add To" function permits votes to be uploaded to counting software multiple times. Id.

V. GIVEN THE UNRELIABLE NATURE OF DREs, STATES AND COUNTRIES HAVE TAKEN STEPS TO PROTECT THE INTEGRITY OF THE VOTE. DEFENDANTS HAVE NOT FOLLOWED THIS TREND OF RESPONSIVENESS.

Defendants' failure to take appropriate action to protect each vote, in light of overwhelming evidence that DREs are insecure, is out of step with the actions of like officials throughout the world. This section discusses steps taken by legislators, election officials, and courts throughout the nation (and around the world) to ensure that the right to vote is protected within their jurisdictions.

A. Eight States Have Enacted Legislation Requiring Either A Voter Verified Paper Ballot Or Voting Only By Paper Ballot.

1. Five States Have Recently Enacted Legislation Requiring DREs To Produce A Voter Verified Paper Ballot For Voter Verification And/Or Recount Purposes.

a. Alaska:

(c) The director[47] shall provide for a paper record of each electronically generated ballot that can be
(1) reviewed and corrected by the voter at the time the vote is cast; and
(2) used for a recount of the votes cast at an election in which electronically generated ballots were used.

2004 Alaska Sess. Laws 154 (codified at Alaska Stat. 01.10.070(c) (2004)).

b. California:

On and after January 1, 2006, a city or county may not contract for or purchase a direct recording electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail.

S.B. 1438 2003 Sess. § 19250(b) (Cal. 2004).

As of January 1, 2006, all direct recording electronic voting systems in use on that date, regardless of when contracted for or purchased, shall have received federal qualification and include an accessible voter verified paper audit trail. If the direct recording electronic voting system does not already include an accessible voter verified paper audit trail, the system shall be replaced or modified to include an accessible voter verified paper audit trail.

---

47 "The director" is a supervisor of elections appointed by the state's lieutenant governor's office. Alaska Stat. § 15.10.105 (2004).

Id. at § 19250(c). The legislation defines "voter verified paper audit trail" as:

> a component of a [DRE] that prints a contemporaneous paper record copy of each electronic ballot and allows each voter to confirm his or her selections before the voter casts his or her ballot;

Id. at § 19251(c). The legislation defines "paper record copy" as:

> an auditable document printed by a voter verified paper audit trail component that corresponds to the voter's electronic vote and lists the contests on the ballot and the voter's selections for those contests;

Id. at § 19250(e). Finally, California's legislation "specifies that a 'paper record copy' is not a ballot." Id.

c. Maine:

> The state may not purchase or approve direct recording electronic voting machines . . . at any time prior to March 1, 2005.

2003 Me. Laws 651, *8. The Maine Laws define "direct recording electronic voting machine" as:

> A system that records votes by means of a ballot display provided with mechanical, electro-optical or electro-audio components that can be activated by the voter, that processes data by means of a computer program and that records voting data in memory components. A direct recording electronic voting machine produces a tabulation of the voting data stored in a removable memory component and on a printed copy.

Id. at *1. The legislation further provides that voting machines:

> [M]ust produce or employ permanent paper records of the votes cast that are able to be verified by individual voters before their votes are cast and that provide a manual audit capacity for the machine. In the case of direct recording electronic voting machines, those records must also identify the individual machines that produced them without revealing the identities of the voters who cast the ballots. In all cases, these records must be reviewed in the event of a recount and considered in conjunction with the machine-produced tally. _____

Id. at *7.

d. Ohio:

> On and after the first federal election that occurs after January 1, 2006, unless required sooner by the Help America Vote Act of 2002, if the voting machine is a direct recording electronic voting machine, it shall include a voter verified paper audit trail.

Ohio Rev. Code Ann. § 3506.10(P) (Anderson 2004). The Ohio code further defines "voter verified paper audit trail" as:

> [A] physical paper printout on which the voter's ballot choices, as registered by a direct recording electronic voting machine, are recorded. The voter shall be permitted to visually or audibly inspect the contents of the physical paper printout . . . After the physical paper printout is produced, but before the voter's ballot is recorded, the voter shall have an opportunity to accept or reject the contents of the printout as matching the voter's ballot choices. If a voter rejects the contents of the physical paper printout, the system that produces the voter verified paper audit trail shall invalidate the printout and permit the voter to recast the voter's ballot.

Id. at § 3506.01(H).

e. Oregon:

Oregon law provides that election recounts "shall be conduct[ed]. . . by hand." Or. Rev. Stat. § 258.211 (2) (2003). Oregon's Secretary of State has interpreted this statute to prohibit DREs that do not produce a "voter verified paper record of each vote cast." Bill Bradbury, Electronic Voting is Trustworthy in Oregon.[48]

2. Three States Require That All Votes, Including Those Cast In The November 2004 Election, Be Cast On Paper Ballots.

a. Illinois:

Illinois law now requires that all votes be cast on paper ballots:

> In all elections hereafter to be held in this state for public officers, the voting shall be by ballots printed and distributed at public expense as provided in this article and no other ballots shall be used.

10 Ill. Comp. Stat. 5/16-1 (2004).

b. New Hampshire:

New Hampshire has passed legislation requiring all votes to be cast on paper ballots:

> [N]o voting machine or device shall be used in any election in this state unless it reads the voter's choice on a paper ballot . . .

---

48 Available at http://www.sos.state.or.us/executive/speeches/110603op.htm (Nov. 6, 2003).

N.H. Rev. Stat. Ann. 656:41 (2004).[49]

c. Vermont:

No voting shall occur in any general election which does not use printed ballots.

Vt. Stat. Ann. tit. 17, 2478 (2003).[50]

B. A Number Of Other Jurisdictions Have Taken Steps To Prevent The Use Of Any DREs That Lack Strict Security Features, Including Voter Verified Paper Ballots.

1. In California, The Secretary Of State Decertified Certain DREs.

As discussed above, under California law, all DREs must produce voter verified paper ballots by 2006. In the interim, California has instituted stringent measures to protect the integrity of the vote. In April 2004, the Secretary of State of California, Kevin Shelley, decertified and withdrew approval of certain DRE voting machines that California had already purchased.

---

49 The Secretary of State of New Hampshire stated that DREs are simply too insecure to be entrusted with the right to vote. Rachel Konrad, Computer miscounts? Not likely in New Hampshire, Associated Press, available at http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2004/01/28/national1609EST0710.DTL&type=printable (Jan. 28, 2004).

50 Vermont enacted this statute after state officials and citizens raised concerns that DREs were insecure. See Matt Sutkoski, Bill Addresses Voting Accuracy, Burlington Free Press, Feb. 7, 2004, at 1B.

The decertification was based on two critical studies of DREs written after the March 2004 Presidential Primary in which multiple problems with the machines were reported. Decertification and Withdrawal of Approval of AccuVote-TSx Voting System as Conditionally Approved November 20, 2003, and Rescission of Conditional Approval, and Decertification_ and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems.[51] The studies examined the DREs' software testing and certification, the machines' reliability and accuracy, the training of poll workers, and the overall security.

The report concluded that DREs were too insecure to use because they were technologically deficient; they could be tampered with easily; they did not provide for meaningful recounts; they did not produce a voter verified paper ballot; and they were not accessible to the disabled.

---

[51]Office of the Sec'y of State of Cal., Decertification and Withdrawal of Approval of AccuVote-TSx Voting System as Conditionally Approved November 20, 2003, and Rescission of Conditional Approval, available at http://www.ss.ca.gov/elections/ks_dre_papers/decert.pdf; http://www.ss.ca.gov/elections/ks_dre_papers/decert.pdf;Office of the Sec'y of State of Cal., Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems, available at http://www.ss.ca.gov/elections/ks_dre_papers/decert1.pdf. http://www.ss.ca.gov/elections/ks_dre_papers/decert1.pdf

The Secretary of State then decertified and withdrew approval of the Diebold AccuVote-TS machines in four counties. He also decertified machines "including but not limited to the AccuVote-TS machines, the ES&S iVotronic, the Sequoia Pacific AVC Edge, and the Hart eSlate." Id. Two of these rejected models, the ES&S iVotronic and Sequoia Pacific AVC Edge, are scheduled to be used in New Jersey in the November 2004 election.[52] Sussex County has 361 ES&S iVotronic machines. NJ Voting Equipment Inventory as of

---

52 Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004, at http://www.njelections.org/voting_machine_co_list_doe.html.

March 2004. Salem County has 160 Sequoia Pacific AVC Edge machines. Id.[53]

The California Secretary of State's decision to decertify direct recording electronic voting machines was upheld by a United States District Court in California. Am. Ass'n of People with Disabilities v. Shelley, 324 F. Supp. 2d 1120, 1131-32 (C.D. Cal. 2004). In upholding the decertification, the court held that the

---

53 California counties will be permitted to use DREs in the November 2004 election only if they used them previously in the March 2004 primary, and if they were also able to meet 23 additional security requirements. These requirements include: making optional paper ballots available at all polling places; making a permanent record on CD or DVD of all votes cast; parallel monitoring at the polls; instituting federal and state testing and qualification of machines; devising technical security, physical security, and communication plans; ensuring that no software modifications are made past September 17, 2004; instituting additional poll worker training; making DREs accessible to the disabled; imposing penalties for tampering; prohibiting the communication of election results via modem; and removing wireless or internet connections from the machines. Id.

public interest in the accuracy of the vote is paramount. Id. The court also held that the Secretary of State's findings concerning DRE insecurity were reasonable grounds to uphold the decertification of the DREs. Id. at 1127-28.

2. Ohio's Secretary of State Halted Deployment Of All Electronic Voting Machines For The 2004 Election.

Like California, Ohio passed legislation (discussed above) requiring that all DREs be equipped with voter verified paper ballots no later than 2006. In the interim, the Ohio Secretary of State rejected the use of all new DREs in Ohio. Among the DREs rejected by Ohio were ES&S's iVotronic and Sequoia Voting Systems' AVC Edge. J. Kenneth Blackwell, The Process of Implementing HAVA is Critical to Success, Spirit of Citizenship & Democracy, Winter 2004, at 3. A total of 521 of these rejected machines are scheduled to be used in New Jersey on November 2, 2004.[54] Sussex County has 361 ES&S iVotronic machines. NJ Voting Equipment Inventory as of March 2004. Salem County has 160 Sequoia Pacific AVC Edge machines.[55] Id. (The Ohio Study is discussed in greater detail above.)

---

54 Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004, at http://www.njelections.org/voting_machine_co_list_doe.html.

55 For Election Day, Ohio counties will be permitted to use the electronic machines they had purchased prior to the Secretary's directive due to "mitigating strategies [implemented by the State of Ohio] to increase security, as well as to reduce risks." Chansky at 4. Specific details of these strategies or plans for

3. The State Of Nevada Requires That All Sequoia Voting Systems DREs Provide An Accessible Voter Verified Audit Paper Trail.

This Election Day, each of Nevada's 329 polling sites will have at least one AVC Edge recently retrofitted by Sequoia Voting Systems to produce a voter verified paper ballot, for all voters who wish to see physical evidence of their votes. Telephone conversation between Nicole Crifo, Rutgers Law Student, and Pat Grenier, Clark County Election Department, October 11, 2004. Busier polling sites may have multiple DREs that produce voter verified paper ballots on hand. Id. All AVC Edge machines in Nevada are required to be retrofitted to produce voter verified paper ballots by the 2006 election. Id.

4. The State Of Maryland Took Action To Remedy Security Vulnerabilities.

As discussed extensively above, three reports written by computer science experts severely criticized the vulnerabilities associated with the DREs the State of Maryland had purchased. Those reports, the Hopkins Report, SAIC, and the RABA Report, made very clear that Maryland's DREs were vulnerable to tampering and so insecure that they could not be trusted for use in an election.

As a result, Maryland overhauled its DREs. It implemented sweeping security changes, including continuous testing of

---

their implementation have not been made available to Plaintiffs at this point.

software of DREs, and employed independent experts to implement remedial suggestions made by the computer experts who prepared the three Maryland reports.[56]

5. New York City Rejected Sequoia Pacific AVC Advantage Machines.

New York City entered into a $60 million contract with Sequoia Voting Systems (then known as Sequoia Pacific) for 7,000 DREs in 1993. Frank Lombardi, Suit Aims To Rescue Electronic Voting, Daily News, Mar. 24, 1996, at 28. The 1993 contract was contingent on the machines' satisfying certain security standards. Id. The machines were Sequoia Pacific AVC Advantage machines. Certif. of Douglas Kellner ¶ 1. Members of the State Board of Elections refused to certify Sequoia's machines, alleging concern over possible security issues with the machines. Lombardi, Suit Aims to Rescue Electronic Voting, at 28.

The City's Department of Citywide Administrative Services rejected a design report submitted by Sequoia Voting Systems as unsatisfactory. Mae M. Chang & Dan Janison, Recount Stirs an Old Debate, Newsday, Sept. 17, 1997, at A05. Sequoia Voting Systems sued the Board in 1996 because its refusal to approve the machines prevented the City from honoring the contract. Lombardi, Suit Aims to Rescue Electronic Voting, at 28. Finally, the contract

---

56 Maryland voters filed suit to seek even further protections and upgrades. The Court denied their request for relief, finding that the State of Maryland had acted responsibly by taking actions to remedy the security deficits. Schade v. Maryland Board of Elections, Memo. Op. Case No. C-04-97297 (Md. 2004).

was canceled in 2000 "after a protracted dispute over [Sequoia's machine] software." Thomas J. Lueck, City Unlikely To Change Voting Gear By November, N.Y. Times, Feb. 9, 2001, at 6.

In a letter to then-Mayor Guiliani, New York City Board of Elections Commissioner Douglas Kellner concluded that DREs were too vulnerable to tampering to be trusted. Election results could be manipulated, Kellner warned.

> The long term security implications of computer voting is staggering to the very essence of our democracy. . . . Nearly every expert who has examined the security issue reports that . . . it would be possible to rig the programming of the machines so that votes would be recorded differently from the way voters intended them to be cast. Even worse, unlike the theft that banks' [sic] occasionally experience in electronic funds transfers, no one would even know that votes were stolen.
>
> The Board of Election has already voted on two separate occasions not to proceed with . . . the Sequoia Pacific Electronic Voting Contract until all of the security issues are satisfactorily resolved. It is becoming increasingly apparent that it will be impossible to provide a level of security which will guarantee the integrity of the electronic voting machines.

Kellner Certif. Exhibit A, Letter from Douglas Kellner, New York City Board of Elections, to Rudolph Guiliani, Mayor, City of New York, June 8, 1995. New York City rejected the use of DREs, and to this day still uses mechanical lever voting machines. Kellner Certif. ¶ 3.

6. The Government Of Ireland Dismantled Its Electronic Voting Machines.

The Irish government appointed the Commission on Electronic Voting to report on the secrecy, accuracy, and testing of the electronic voting system to be used in the June 2004 local and European elections. Ireland Commission on Electronic Voting, Interim Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System 7 (Apr. 29, 2004). The Commission's investigation took two months. Id.

Six weeks before the election, the Commission recommended the rejection of all electronic voting machines. This recommendation was not based on any conclusive finding that the electronic voting machines were certain to malfunction on Election Day. Rather, its recommendation was based on the failure of the machines to satisfy the basic standards for security and reliability. Id. The Government of Ireland adopted the Commission's recommendations and retired the DREs. Id.

7. The Supreme Court Of Venezuela Enjoined The Use Of All Electronic Voting Machines Scheduled To Be Used In The 2000 General Election.

Two days before the 2000 election, the largest in Venezuela's history, the Supreme Court postponed the election because of problems with the installed ES&S software. Associated Press, Venezuela Using Untested Voting Machines, ABC News 7 (July 11,

2004).[57] The machines scheduled to be used in the election were ES&S's iVotronics.[58] In New Jersey, Sussex County is currently scheduled to employ 361 iVotronic machines in the November 2004 election.[59]

In its August 2004 presidential recall election, Venezuela used DREs, which were manufactured by Smartmatic and produced a voter verified paper trail. David Isaac, E-Voting Machines Spread Fast, But Critics Say Security Lacking, Investor's Business Daily, Oct. 5, 2004, at A01. President Chavez kept his office after the election results were confirmed by an audit led by the Carter Center. Id.

VI. NEW JERSEY CITIZENS AND LEGISLATORS HAVE EXPRESSED THEIR MOUNTING CONCERNS OVER THE INHERENT INSECURITY OF DREs TO ATTORNEY GENERAL HARVEY AND GOVERNOR MCGREEVEY. THESE CONCERNS HAVE BEEN IGNORED.

---

57 Available at http://www.wjla.com/news/stories/0704/158551.html (July 11, 2004).

58 ES&S in the News – A Partial List of Events, at http://www.votersunite.org/info/ES&Sinthenews.pdf.

59 Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004, at http://www.njelections.org/voting_machine_co_list_doe.html.

Plaintiffs and other citizens across the State of New Jersey have expressed their concern about the unreliability of DREs that lack a voter verified paper ballot to Governor McGreevey and Attorney General Harvey. Both Defendants have failed to respond to repeated requests by New Jersey citizens to institute security measures to protect their votes.

Only New Jersey legislators have been responsive to voters. Two New Jersey Legislators, New Jersey Assemblyman Reed Gusciora and U.S. Congressman Rush Holt have sponsored legislation in the New Jersey Assembly and U.S. House of Representatives, respectively, to ensure that every vote is counted when voters go to the polls.

In May 2004, Plaintiff Assemblyman Gusciora proposed Assembly Bill No. 2627, 211th Leg. (N.J. 2004)(proposed), which would amend N.J.R.S. 19:48-1 and P.L. 1973, c.82 to include a requirement for an individual "permanent paper record for each vote cast" that would be "made available for inspection and verification by the voter" and could be "preserved for later use in any manual audit." A.2627, 211th Leg. §§ 1(o) and 3(I).[60] He also co-sponsored a

---

60 Assemblyman Gusciora's bill is modeled after federal legislation proposed by U.S. Congressman Rush Holt. Congressman Holt's bill, introduced in May 2003, would require voter verified paper record of votes cast on DREs nationwide. The Voter Confidence and Increased Accessibility Act of 2003, H.R. 2239 IH, 108th Cong. §§ 1 and 4(a)(2)(A)(2003). The intent of this legislation is to promote the "accuracy, integrity, and security" of the voting system. Id. at § 4(a)(2)(A). The legislation calls for a "voter verified permanent paper record" that can be used for a future audit of the election results, as well as an opportunity for the

bill that would improve access to polling sites for disabled and elderly voters. Assembly Bill No. 2629, 211th Leg. (N.J. 2004)(proposed).

Assemblyman Gusciora, concerned that his proposed legislation would not protect voters this Election Day, has tried in vain to work with Governor McGreevey and Attorney General Harvey to make sure that voters are protected this November. He has requested that both Attorney General Harvey and Governor McGreevey issue executive orders to make paper ballots available this November.

Assemblyman Gusciora wrote a letter on June 16, 2004, to Attorney General Harvey identifying the serious problems associated with DREs. In his letter, Assemblyman Gusciora also discussed that many reports have identified the serious problems associated with electronic voting machines, and listed the concerns that led him to introduce legislation that protects the voters' intent. Assemblyman Gusciora then requested from Attorney General Harvey plans to ensure the integrity of the upcoming election. Letter from Reed Gusciora (D), State of New Jersey

---

voter to correct errors before the paper ballot is preserved. Id. at § 4(a)(2)(B)(i)-(ii).

The proposed legislation also mandates that no voting systems use secret, undisclosed software or source code, or contain a wireless communications device. Id. at § 4(a)(2)(C)(i)-(iii). The legislation also requires certification for all electronic voting systems with respect to the foregoing requirements. Id. at § 4(a)(2)(C)(i)-(iii). Congressman's Holt's legislation is supported and co-sponsored by four other New Jersey Congressmen: Congressman Frank Pallone (NJ-6), Congressman Bill Pascrell (NJ-8), Congressman Donald Payne (NJ-10), and Congressman Steve Rothman (NJ-9), as well as more than 150 other bipartisan cosponsors.

Assemblyman, Leg. District 15, to Peter Harvey, Attorney General, State of New Jersey (June 16, 2004)(hereinafter, "Gusciora Letter"). (The Gusciora Letter is attached to Plaintiffs' Complaint as Exhibit A.) Attorney General Harvey has not responded to Plaintiff Assemblyman Gusciora's concerns.

In addition to Assemblyman Gusciora, Mercer County Executive Brian M. Hughes has voiced his concern regarding the use of electronic voting machines that produce no voter verified paper ballot. Letter from Brian M. Hughes, Mercer County Executive, State of New Jersey, to Peter Harvey, Attorney General, State of New Jersey, July 22, 2004 (hereinafter, "Hughes Letter"). (The Hughes Letter is attached to Plaintiffs' Complaint as Exhibit B.) In his July 22, 2004 letter to Attorney General Harvey, County Executive Hughes stated that he is in support of Congressman Holt's legislation. Id. Accordingly, he secured funds to retrofit with features that would provide a verified paper ballot the 600 Sequoia Voting Systems machines already purchased by Mercer County. Id. County Executive Hughes notified Attorney General Harvey of his frustration with Sequoia Voting Systems, which refused to retrofit the machines before Election Day. Id.

To preserve the integrity of the vote in Mercer County, County Executive Hughes requested the support of Attorney General Harvey to obtain an executive order to allow "voters to use absentee ballots if they lack confidence in the electronic system." Id. The request for an executive order was denied.

Concerned citizens throughout the State have also attempted to bring their concerns regarding DREs to the attention of Governor McGreevey and Attorney General Harvey. Plaintiffs, as part of a coalition of advocacy groups, also expressed their concerns about DRE inadequacies to Governor McGreevey and Attorney General Harvey in July 2004. This coalition collected over 20,000 signatures from New Jersey voters "who oppose electronic voting machines that do not produce voter-verifiable paper trails." Certif. of Beth Feehan ¶ 2 (Oct. 14, 2004).

The signatures collected were presented to members of Governor McGreevey's staff, following a "National Day of Action" sponsored by True Majority on July 13, 2004. Id. at 4. The rally and press conference took place on the State House steps in Trenton. Id. at 3. Plaintiff, Coalition for Peace Action, as well as other advocacy groups such as Common Cause, Democracy for America, Verified Voting, Rock the Vote, and Computer Professors for Social Responsibility, co-sponsored the event. Id. Speakers included Plaintiff Assemblyman Reed Gusciora, Professor Edward Felton of Princeton University, and Reverend Bob Moore of Plaintiff Coaltion for Peace Action.[61] Unfortunately, the Governor again failed to respond to the public's concerns.

On August 27, 2004, Governor McGreevey and Attorney General Harvey were presented with a letter signed by 22 public interest

---

61 Computer Ate My Vote, Coalition for Peace Action, available at, http://www.peacecoalition.org/action/2004Q3/040713_verified_voting.html (last visited Oct. 14, 2004).

organizations and individuals, including Plaintiff Assemblyman Gusciora and Reverend Bob Moore on behalf of Plaintiff Coalition for Peace Action.[62] The letter discussed "inadequate certification processes, secret source codes and software, and the lack of security" surrounding the electronic voting machines. Letter from Renee Steinhagen, New Jersey Appleseed PILC, et al., to James McGreevey, Governor, State of New Jersey, Aug. 27, 2004 (hereinafter, "Advocates Letter") (The Advocates Letter is attached to Plaintiffs' Complaint as Exhibit C.). The Advocates Letter calls on the Governor and the Attorney General to issue an order to make paper ballots available at all polling sites to anyone who wishes to use them. Id.

The Advocates Letter points out that making paper ballots available to all voters is entirely doable, as other states, including California, have implemented this policy. Id. As the

---

62 The Advocates Letter was signed by the following persons/advocacy groups: Stephen Flatow, Community Relations Committee, United Jewish Community of MetroWest; Assemblyman Reed Gusciora, District 15; Ben Cohen, True Majority; Ed Davis, Common Cause; Peter Schurman, MoveOn.org; Cindy Cohn, Electronic Frontier Foundation; Pamela Smith, VerifiedVoting.org; Craig Kaplan, American Families United, Voter Protection Project; Margaret Fung, Asian American Legal Defense Education Fund; Gary Ferdman, Business Leaders for Sensible Priorities; Laurie Lowenstein, NJ Coalition for Democracy; Cynthia Sheward, Records Manager, Clinton, NJ; Susan Waldman, Morris County NOW; Rev. Bob Moore, Coalition for Peace Action; Alan Sagner, Alan Sagner Companies; Joshua W. Denbeaux, Esq., Debeaux & Denbeaux; Rebecca Mercuri, Ph.D., Computer Scientist; Edward Felton, Ph.D., Princeton University; Mindy Kleinberg, 9/11 Family Steering Committee; Lorie Van Auken, 9/11 Family Steering Committee; and Alison Miller, West Windsor Town Council. The Advocates Letter was copied to Attorney General Peter Harvey, among others.

letter points out, issuing such an executive order in New Jersey "would involve no change in statute, cause minimum confusion among election officials . . . and create minimal additional costs for printing more emergency ballots than usual." Id. Unfortunately, to the dismay of the concerned citizens, the Governor and the Attorney General have not responded to the requests and concerns of these individuals.

Most recently, Counsel for the Plaintiffs, Penny M. Venetis, Esq., of the Rutgers Law School Constitutional Litigation Clinic, sent a letter of concern to Attorney General Harvey, addressing the many risks associated with electronic voting across the country and particularly in New Jersey. Letter from Penny M. Venetis, Esq., to Peter Harvey, Attorney General, State of New Jersey, Oct. 1, 2004 (hereinafter, "Venetis Letter").[63] (The Venetis Letter is attached to Plaintiffs' Complaint as Exhibit D.)

In her letter, Ms. Venetis described many of the reasons (which are also detailed in this brief) that electronic voting systems are unreliable, unsafe, and untrustworthy for the upcoming election. Id. Ms. Venetis recommended that the Attorney General order the use of paper ballots for voting this Election Day. Id. She also asked him to order that all existing machines be retrofitted to create a voter verified paper ballot, and that all machines purchased in the future be required to have paper ballot verification components. Id. Finally, Ms. Venetis requested a

63 This letter was copied to Donna Kelly, Esq., Deputy Attorney General, State of New Jersey.

meeting with Attorney General Harvey to discuss the concerns raised in her letter. Id. She followed-up her letter with telephone calls to the Attorney General's office. The Attorney General has not responded to her letter or calls.

The inaction and lack of response by the Governor and Attorney General necessitates that this Court step in to ensure that every vote is counted accurately on Election Day. The DREs scheduled for use this Election Day simply cannot be trusted with our precious right to vote.

ARGUMENT

I. ELECTRONIC VOTING MACHINES POSE A GRAVE RISK TO NEW JERSEY VOTERS' CONSTITUTIONALLY-PROTECTED RIGHT TO VOTE.

The right to vote is enshrined in the New Jersey Constitution, and has been recognized as fundamental by the Supreme Courts of New Jersey and the United States. Because it is so fundamental, and so strongly protected by State law, this Court should take immediate action to ensure that every vote will be counted on Election Day.

It is impossible to predict whether or not any DREs scheduled for use on Election Day will malfunction on Election Day. The right to vote, however, is too precious to subject to the vulnerabilities of DREs. DREs and ancillary tabulation equipment have extensive histories of malfunctioning across the nation, both while being tested and during actual elections. These malfunctions included a failure to count votes. The loss of even one vote is anathema to the New Jersey Constitution.

Because of the severity of the constitutional deprivation which would occur from malfunctioning electronic voting machines, this Court should enjoin the use of all DREs in the upcoming election, and should require that every citizen who wishes to vote, vote by emergency paper ballot, as described in N.J.S.A. 19:53B-1, or by absentee ballot, as described in N.J.S.A. § 19:57-1. Absentee ballots can be scanned using optical scan machines that almost all New Jersey counties have used for decades.

This Court should further require that, after the election, all DREs be retrofitted with devices capable of producing voter-verified paper ballots using the "Mercuri Method." See Mercuri Certif. 42. Such ballots provide for independent audits of each vote in the event of a malfunctioning DRE or a recount. The relief sought here is necessary in order to protect the fundamental rights of New Jersey voters.

A. The Right To Vote Is One Of The Most Stringently Protected Rights Under The New Jersey And Federal Constitutions.

> Article II, § 1, ¶ 3(a) of the New Jersey Constitution states: Every citizen of the United States, of the age of 18 years, who shall have been a resident of this State and of the county in which he claims his vote 30 days, next before the election, shall be entitled to vote for all officers that now are or hereafter may be elective by the people, and upon all questions which may be submitted to a vote of the people[.]

The New Jersey Supreme Court has long recognized that the right to vote, guaranteed by Article II, § 1 of the New Jersey Constitution, is one of the most fundamental and important rights

in a democratic society. See Gangemi v. Berry, 25 N.J. 1, 12 (1957). As Chief Justice Weintraub eloquently explained,

> ...[d]espite an impoverished beginning, the right to vote has taken its place among our great values. Indeed the fact that the voting franchise was hoarded so many years testifies to its exalted position in the real scheme of things. It is the citizen's sword and shield. 'Other rights, even the most basic, are illusory if the right to vote is undermined.' It is the keystone of a truly democratic society.

Gangemi v. Rosengard, 44 N.J. 166, 170 (1965) (quoting Wesberry v. Sanders, 376 U.S. 1, 17 (1964)).

More recently, in New Jersey Democratic Party, Inc. v. Samson, the New Jersey Supreme Court again affirmed the principle that voting is a fundamental right of New Jersey citizens. 175 N.J. 178 (2002). Chief Justice Poritz, writing for a unanimous Court, stated that "[w]hen this court has before it a case concerning the New Jersey election laws, we are directed by principle and precedent to construe those laws so as to preserve the paramount right of the voters to exercise the franchise." Id. at 190. The Chief Justice explained that the "fundamental right to exercise the franchise infuses our election statutes with purpose and meaning." Id. at 186. In keeping with that purpose, the Court found that the statutory deadline for ballot changes could be extended to ensure that voters were presented with legitimate choices on Election Day. Id. at 199.

In Samson, the Democratic party sought to change the ballot after the deadline had passed, replacing one candidate's name with another. Id. at 184. The court held that, despite the deadline

expiration, the change could be made to preserve the voters right to choose a candidate and maintain the established two party political process in this country. Id. at 198-99. New Jersey's broad protection of the right to vote is further illustrated by In Re Absentee Ballots Cast By Five Residents of Trenton Psychiatric Hospital, 331 N.J. Super. 31 (App. Div. 2000). Despite a constitutional provision that denies voting rights to "idiots" or the "insane", the Appellate Division found that a per se finding of incompetence for those committed to mental institutions was inconsistent with New Jersey's "overriding public policy in favor of enfranchisement." Id. at 35-36. The Court found that "[s]uch policy derives from the basic precept that the right to vote is quintessential to our democratic process." Id. at 36 (citing Gangemi, 25 N.J. at 12).

The United States Constitution also protects the rights of citizens to vote in both state and federal elections. Reynolds v. Sims, 377 U.S. 533, 554-55 (1963). The right to vote freely is the "essence of a democratic society, and any restrictions on that right strike at the heart of representative government." Id. at 555. The United States Supreme Court has consistently recognized the right to vote as a fundamental one. "Undoubtedly, the right of suffrage is a fundamental matter in a free and democratic society." Reynolds, 377 U.S. at 561-62. "Almost a century ago . . . the Court referred to 'the political franchise of voting' as 'a fundamental political right, because [it is] preservative of all

rights.'" Id. at 562 (quoting Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886)).

Because of the special esteem granted to the franchise, it receives special protection: "Especially since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." Reynolds, 377 U.S. at 562.

B. The Fundamental Right To Vote Requires That The True Intention Of The Voter Is Recorded.

In New Jersey, "[e]lection laws are to be liberally construed so as to effectuate their purpose." Kilmurray v. Gilfert, 10 N.J. 435, 440 (1952). The right to the franchise includes more protection than simply the right to cast a ballot. "'The right to vote includes the right to have the ballot counted.'" Reynolds, 377 U.S. at 555 n.29 (quoting South v. Peters, 339 U.S. 276, 279 (1950) (Douglas, dissenting)). Under the New Jersey and Federal Constitutions, the true intention of the voter must be considered, and respected by election officials and courts.

For example, in In Re General Election Held in the Township of Monroe, the Appellate Division decided to interpret liberally New Jersey voting law to capture the true intention of the voters. 245 N.J. Super. 70 (App. Div. 1990). In Township of Monroe, voters in a district cast their vote for mayor by both marking his name printed on the ballot and by writing in his name in the write-in

portion of the card. Id. at 71. These votes were not counted initially because they allegedly violated N.J.S.A. 19:53A-7(f)(2004) which states: "[i]f the voter has cast more votes for an office than he is entitled to vote for, the vote for that office shall be declared null and void and that vote shall not be counted for that office." Id.

The Appellate Division rejected that rigid interpretation of the statute. The court found that by voting for the same candidate in two places on the ballot the voters did not truly violate this law, and ordered that the votes be counted. Id. at 73. "A contrary ruling would result in disenfranchising voters who clearly demonstrated an intent to vote for one particular person for one particular office." Id. See also In Re the Petition of Gray-Sadler, 164 N.J. 468 (2000)(setting aside an election where write-in votes were not counted due to poor instructions at the polls, despite the voter's clear intentions); In Re the Petition of Fifteen Registered Voters of the County of Sussex, 129 N.J. Super. 296 (App. Div. 1974)(write-in votes counted where voters used only a first initial or only the last name when identifying their selection).

As demonstrated by these cases, New Jersey courts have consistently equated the right to vote with the requirement that the true intent of the voters be captured.

1. DREs Are Inherently Insecure And Cannot Be Relied Upon To Accurately Record The Intent Of New Jersey Voters.

DREs throughout the United States have malfunctioned. The machines have even malfunctioned during public tests organized by manufacturers, ironically to instill voter confidence. Kim Zetter, Wrong Time For an E-Vote Glitch, Wired News.[64] The track record of DREs is simply too tenuous to be entrusted with the fundamental right to vote.

As detailed above, in Boca Raton, Florida, malfunctioning DREs have attributed votes cast for one candidate to his opponent. Olson, Out of Touch. Glenn Cantor also experienced the same thing. The DRE he used in Mercer County switched his choice when he pressed the "CAST VOTE" button. Cantor Certif. at 8. Voter intent is obviously not captured when such a malfunction occurs. The voter is robbed of her constitutional right to cast her ballot for a preferred candidate.

In other instances, in Broward and Palm Beach Counties, Florida; Natrona County, Wyoming; Hillsborough County, Florida; Dallas, Texas; and Riverside County, Florida, votes cast on DREs have been lost, either by the machines themselves or by tabulating software. Bolstad, New System No Easy Touch for 134 Voters in Broward; Olson, Out of Touch; Van Dusen; Clerk Changes Election Vote Totals; Testerman, Voting Mystery Stirs Call for Paper Trail; Ackerman, Electronic Voting's Hidden Perils.

When DREs fail to record votes, or register votes as being cast for the wrong candidate, then the voter's true intention is

---

64 At http://www.wired.com/news/evote/0,2645,64569,00.html?tw=wn_tophead_2 (Aug. 12, 2004).

lost. Because Attorney General Harvey and Governor McGreevey refused to issue executive orders requiring that DREs in New Jersey produce a voter verified paper ballot, voter intent can never be ascertained. This is of particular concern in the event of a machine malfunction or a recount, where there is no independent way to determine the veracity of an electronic voting machine's tabulation.

2. The Certification Process For Voting Machines Contained In Title 19 of New Jersey Statutes Does Not Provide Any Assurance That DREs Will Count Votes Accurately.

a. DREs Are Not Contemplated In Any Respect By Current New Jersey Law Governing Certification Of Voting Machines.

Title 19 of the New Jersey Statutes lays out the requirements for elections in the State, including the process for certifying voting machines. The statute clearly states that all voting machines must be certified before they are used in an election. N.J.S.A. 19:48-2, 19:53A-4. The statute, however, is completely silent as to DREs.

There is absolutely no directive for certifying DREs. Existing New Jersey law assumes that electronic voting machines will be used only to count paper ballots! For example, N.J.S.A. §§ 19:53A-1 et seq. defines an electronic voting machine as one "in which votes are recorded on ballot cards, and such votes are subsequently counted and tabulated by automatic tabulating equipment at one or more counting centers." N.J.S.A. 19:53A-1(e)

(emphasis added). "Automatic tabulating equipment" is defined as an "apparatus which automatically examines and counts votes recorded on ballot cards, and tabulates the results." N.J.S.A. § 19:53A-1(a)(emphasis added). Chapter 53A governs the physical requirements of optical scan machines only, and does not contemplate the use of other types of electronic voting systems such as DREs.

It is true that N.J.S.A. § 19:53A-2(b) states that the Act's provisions "shall be controlling with respect to elections where electronic voting systems are used, and shall be liberally construed so as to carry out the purpose and intent of this act." But, this language is not an endorsement of DREs. N.J.S.A. 19:53A-2(b) must be read in the context of the entire statute. As described above, the language of Chapter 53A describes electronic voting machines as devices that count paper ballots. DREs are too different from optical scanners to be construed as electronic voting systems within the meaning of N.J.S.A. § 19:53A et seq. To hold otherwise is to excuse the State from its obligation to ensure that voting machines be secure and reliable at the time they are used in an election.

b. The Testing Committee Contemplated By Title 19 Does Not Guarantee Proper Certification of DREs.

N.J.S.A. 19:48-2 requires the certifying authority (previously the Secretary of State, now the Attorney General) to have a voting machine undergoing certification examined by a committee of three experts, "one of whom shall be an expert in patent law and the

other two mechanical experts." Those experts must submit a written report about the machine.

This requirement is insufficient for DREs. DREs are not mechanical machines. Thus, review and certification by the committee of experts under current New Jersey law does not necessarily provide the type of stringent review contemplated by Title 19. There is no requirement, or guarantee, that the committee will possess the "appropriate quality assurance and computer security skills needed to evaluate the accuracy, integrity, reliability, and auditability of DRE voting systems." Mercuri Certif. 30. Testing must be conducted by "electrical engineers and computer scientists" who can appreciate the complexities of DRE technology. Appel Certif. 63. Patent law and mechanical experts will not be able to properly review "the overwhelming majority of the complexity of a DRE machine," which is found "in the electronic circuits and . . . computer software." Appel Certif. 63.

Even if a computer expert were used to review DREs,[65] the certification process would still be flawed. A one-time review of a DRE cannot ensure that the specific machine inspected will function properly. It is necessary that the machines be constantly reviewed. Appel Certif. 59, 60. Testing must be far more

---

65The Division of Elections, according to the HAVA-NJ State Plan, employs "a patent attorney, one voting machine expert and an information technology expert." HAVA-NJ State Plan 24. It is unclear what an "information technology expert" is. Plaintiffs' attempts to secure any information about the committee that certifies DREs have been fruitless.

comprehensive, in order to locate all of the potential errors associated with a DRE. Appel Certif. 26; Mercuri Certif. 31.

c. The Attorney General Has Admitted That DRE Technology Has Outpaced New Jersey's Certification Statutes.

Attorney General Harvey admits that DRE technology has "outpaced" our State's laws protecting voters and the election process. HAVA-NJ State Plan 25. Yet neither Attorney General Harvey nor Governor McGreevey have taken proper action to protect the right to vote from being compromised by untested DREs.

The Attorney General's website lists certain models of DREs, and states that these machines have been certified. Certified Voting Machine/Devices in New Jersey. It is from this list of machines that counties are instructed to choose when they are buying DREs. This endorsement of DREs as being certified is erroneous. As discussed above, New Jersey's statutes governing election law do not contemplate DREs. Thus, the DREs endorsed by the Attorney General have not passed the rigorous testing Title 19 intended voting machines to undergo before they are used.

DREs on the Attorney General's list are allegedly approved by the National Association of State Election Directors ("NASED"), in accordance with HAVA. Voting Systems That Are NASED Qualified.[66] Nowhere in Title 19 does it state that any form of federal certification is a substitute for independent New Jersey certification. As discussed above, Ohio, California, Maryland,

66Available at http://www.nased.org/NASEDApprovedSystems1.03.pdf (Jan. 3, 2003).

Georgia, Texas, and Florida rejected DREs that had been federally certified after they conducted their own examinations of the machines, and realized the machines should not have been state-certified. Appel Certif. 64. The rejection by California and Ohio of the very same machines scheduled to be used in New Jersey on Election Day is discussed above, and is further proof that federal certification alone is insufficient.

Moreover, all DREs purchased through 2003 (which would include the AVC Advantage, AVC Edge, and iVotronic), were certified according to "obsolete" Federal Elections Commission guidelines. Mercuri Certif. 36. Other states have clearly recognized these failings of the federal certification process, and rejected DREs that did not meet their own stringent testing procedures. The Attorney General's failure to conduct "additional testing to mitigate the flaws of the [federal] process" means that any DREs that have been purchased by New Jersey counties likely do not meet the stringent requirements intended for voting machines under Title 19. Id. at 37.

The Attorney General's list of DREs contains the make and model of each voting machine, as well as the year it was allegedly certified.[67] Nowhere in his website does the Attorney General state

---

67 Under HAVA, voting machines are to be tested and certified by "accredited laboratories." Pub. L. No. 107-252, § 231(a), 116 Stat. 1666, 1684-85. These tests can be directed by the federal Election Assistance Commission or the individual states, but they must conducted by the laboratories. Id.

that each new machine purchased by a county must be individually certified.

If this indeed is the method of certification the Attorney General is endorsing - where a machine model, rather than each individual machine, is certified - the method is constitutionally flawed. If one applies this logic to another context, the danger of transitive certification becomes very clear. This method of certification is akin to stating that if one make and model of a single automobile is tested, then all models of that car produced by the manufacturer have also been tested, and never have to undergo individual inspections. See Mercuri Certif. 34, 36. We know that such a blanket endorsement of automobiles would be dangerous, and could lead to the loss of life. In the context of voting, certification in perpetuity of a particular make and model of DRE is constitutionally dangerous, because itcan lead to loss of a fundamental right - the right to have one's vote counted accurately.

The technology of DREs is such that every single machine must be inspected and certified. Appel Certif. 56-62. Examining one machine does not reveal details about every machine, because not all machines are exactly alike. Appel Certif. 56. Examining a single model of DRE will not ensure that the computer program in each machine can be relied upon to count votes accurately. Id. It is absolutely essential that each machine's software function properly, especially when the DRE produces no voter verified paper ballot. Id. Otherwise, given how easy it is to tamper with DREs,

there is a grave risk that the DRE will manipulate votes. Because the Attorney General has failed to order that the software of each DRE be carefully certified, there is no way to know that in fact each DRE will accurately count all votes cast on it.

The lifetime certification of DREs ignores the fact that software is always changing and must be re-checked. We know that the Sequoia Pacific AVC Advantage, which is scheduled to be used by at least 2.8 million registered voters this November, is not the same as the one which the Attorney General claims was certified in 1987. See AVC Advantage Security Overview 5 (2004). The manufacturer literature of the AVC Advantage admits that Sequoia Voting Systems' AVC Advantage has been "significant[ly]" updated since 1987. Id. Both the hardware and the software of the AVC Advantage have been updated since then. Appel Certif. 59-60.

Any software change, even one letter of change, can re-write an entire program and cause a machine to function in a completely different way than the original program authorized. Id. In the context of a DRE, this change can cause the DRE to add, erase, or mis-attribute votes. When "substantive" changes are made to a DRE, it is necessary to revoke any certification and re-test and re-certify the machine. Mercuri Certif. 33; see also Appel Certif. 65.

Proof that the 1987 software is flawed can be found in the dispute between New York City and Sequoia Pacific. In 1993, New York City cancelled its contract with Sequoia Pacific because the AVC Advantage proved to be too unreliable. Lombardi, Suit Aims to

Rescue Electronic Voting, at 28. At least 2.8 million registered voters in eleven New Jersey counties are scheduled to use 6,508 of these very rejected machines on Election Day. NJ Voting Equipment Inventory as of March 2004; Registered Voters as of the Close of Registration for the Primary Election to Be Held on June 8, 2004. Thus, the Sequoia Pacific AVC Advantage is a completely different machine from what was certified in 1987. The Attorney General does not believe this to be significant and continues to endorse the use of this machine. Such blanket endorsement is unwise.

The Sequoia Pacific AVC Edge, which the Attorney General lists as having been certified in 2001, Certified Voting Machine/Devices in New Jersey 3, is also seriously flawed. It has demonstrated its unreliability through its many malfunctions, including missing votes and registering votes for one candidate as being cast for another. Moreover, it has the specific vulnerability of permitting a complete overhaul of its program in less than five minutes! Appel Certif. 50. Yet, the Attorney General endorses this DRE. As discussed above, this DRE was rejected by Secretaries of State of California, Nevada, and Ohio as being too flawed to be entrusted with the right to vote.

At least 40,000 registered voters in Salem County will use this unreliable DRE on Election Day.

The Attorney General's blanket certification system is even more disturbing, because the Attorney General plays fast and loose with his own flawed system of certification. He specifically

endorses DREs that have never been certified, even under his own rules!

The Attorney General admits on his website that the ES&S iVotronic has never been certified in New Jersey. Certified Voting Machine/Devices in New Jersey 3. He endorses it because the iVotronic is allegedly the same as ES&S's EP Votronic. Id. One cannot assume that machines are identical when the manufacturer has called them by different names. Attributing perpetual certification to "similar" machines is even more problematic than attributing certification to machines of the same make and model. As discussed extensively above, many serious problems have been associated with iVotronic machines. They have failed to count votes and have mis-attributed votes. The iVotronic is so insecure that Ohio and California decertified the machines and will not permit them to be used unless they pass stringent security measures. There is thus no justification for the Attorney General's blanket endorsement of this DRE.

As discussed above, Attorney General Harvey has not taken appropriate steps to ensure that all DREs to be used in New Jersey are properly certified. Because the statutory certification process for voting machines cannot be applied to DREs, there is no assurance whatsoever that the DREs endorsed by the Attorney General can be trusted to record votes accurately. This flawed certification process violates the New Jersey Constitution's mandate that every vote be counted accurately.

II. DRES SCHEDULED FOR USE IN NEW JERSEY CANNOT RECOUNT ACTUAL VOTES AS REQUIRED BY LAW. THEIR USE THEREFORE VIOLATES VOTERS' STATUTORY AND CONSTITUTIONAL RIGHTS.

Title 19 of the New Jersey Code is silent about DREs and the requirements necessary to properly recount the votes they are designed to record. As noted above, N.J.S.A. 19:53A, entitled "Electronic Voting," deals exclusively with how optical scanners are used to tabulate votes recorded on paper ballots. The complete lack of guidelines to county election officials with respect to DRE votes can lead to total chaos in the event that a recount is needed this November.

In the event of a recount, each affected county using DREs will be forced to devise its own method for recounting votes. As discussed more fully below, this runs afoul of both the New Jersey Constitution's equal protection guarantees and New Jersey statutory requirements governing recounts.

A. DREs Do Not Allow A "Recount Of Votes Cast At The Election" As Required By New Jersey Statutes.

Title 19 of the New Jersey Code lays out detailed instructions for the recount of paper ballots, ballot cards and lever-cast votes. In contrast, no instructions are given on how to perform recounts of votes cast using DREs.

N.J.S.A. 19:28-1 provides that a candidate who believes an error has been made may apply to a judge of the Superior Court for a recount. If the judge determines that a recount is necessary,

the judge orders a public recount by the county elections board in the judge's presence. N.J.S.A. 19:28-3.

The judge determines the terms under which the recount is conducted, and decides any disputed questions that cannot be resolved by a majority vote of the county board of elections. Id. The elections board attends the recounting under subpoena, "witness[es] the opening of the ballot box or boxes," and may subpoena witnesses and evidence. Id. Each ballot box used in the recount contains all ballots cast, spoiled, unused or rejected at the election, as well as one tally sheet, as provided in N.J.S.A. 19:18-1 (Election records placed in ballot box).

Similarly, votes cast in an optical-scan system (used for all ballots in Warren County, and for provisional and absentee ballots in most other counties) are recounted by repeating the optical scanning process described in N.J.S.A. 19:53 A-8. This includes producing duplicates for defective ballot cards (as necessary), and counting some or all votes manually if the county board of elections determines it is impracticable to complete the count mechanically. Additionally, a court may order a manual recount of ballot cards. N.J.S.A. 19:53A-14.

Protocols for rechecking votes cast on lever machines are set forth in N.J.S.A. 19:52-6:

> The judge shall ... order the machine in question opened and the registering counters rechecked against the election officers' returns. ... under the supervision of the county election officials and in co-operation with the parties at interest or their representatives.

The particular "manner of rechecking machines" is spelled out in more detail in N.J.S.A. 19:52-6.1. That statute describes the unpacking and unlocking of the machine, the opening and reading of the counters, the compilation of tally sheets and their comparison to the original election records. See generally N.J.S.A. 19:52-6.1; see also Theurer v. Borrone, 81 N.J. Super. 188, 191 (L. Div. 1963) aff'd 85 N.J. Super. 142 (App. Div. 1964).

Counting votes cast on paper or ballot card, or by physically moving a lever, is a simple process of examining a physical artifact of voter intent. Thus, counting and recounting can be observed easily by the public.

Lever-machine counters, although they produce no paper verification, can still produce very reliable recount information. Counters in lever machines are advanced through a simple, verifiable mechanical process. The physical effects of that process, consisting of the observable movement of the counters, can be easily observed.

> A voter walks up to the machine and pulls a large central lever. This lever both closes a curtain around the voter to maintain privacy and readies the machine to accept a vote. The voter is presented with a lever for each candidate or ticket [or ballot question]. Voters can change their own votes as many times as they want; and when they've made their final decision they pull the central lever back to its original position, which registers their choices, resets the levers, and opens the privacy curtain.
>
> Internally, when the central lever is reset, the voted-on candidate's lever advances a counter. The counter essentially operates like the odometer of a car. Because of their relative internal simplicity, mechanical lever machines are difficult to "rig" because it is obvious

> when one candidate's linkage rod is disconnected or connected to the wrong counter.

William Nicoll, How Things Work - Voting Machines, The Tartan Online.[68]

The relative internal simplicity of a lever machine allowed the Appellate Division to determine that the results of a local election were misreported due to a specific and easily-proven mechanical malfunction. See Application of Moffat, 142 N.J. Super. 217, 222 (App. Div. 1976) (Shaft connected to counter wheel registering votes for a candidate "became dislodged, so that the wheel failed to move after the first vote was cast for him.")

A DRE, in sharp contrast to lever machines, optical scanners and human counters, could take votes cast for candidate "A" and record them as votes for candidate "B" without leaving a trace. See Mercuri Certif. 38. Its subsequent confirmation of its own inaccurate record would be a mere reprint masquerading as a recount. At best, DREs asked to perform a recount will state the same result they stated once before. This is very different from demonstrating that their original statement was accurate. Accepting a reiteration of previous conclusions about electoral results in lieu of a recount is incompatible with New Jersey statutory law.

Additionally, reliance on a vendor's assistance in the event of a recount would be anathema to New Jersey law. A vendor's

---

[68] At http://www.thetartan.org/article.jsp?editionid=26&id=659 (last visited Oct. 15, 2004).

assurances that it should be trusted to accurately process and honestly report electoral data begs the question every recount is designed to answer: whether the votes were recorded accurately in the first place. New Jersey statutes clearly and consistently require visible and tangible proof of voter intent.

Title 19 consistently defines recounts in terms of physical evidence of voter intent. This discussion is effectively identical to the State of Oregon's requirement that recounts be conducted manually. Bill Bradbury, Electronic Voting Is Trustworthy In Oregon, The Oregonian, November 6, 2003.[69] Oregon law requires that all recounts be conducted by hand. Id. Oregon Secretary of State Bill Bradbury interprets that requirement as barring the use of DREs that do not produce a voter verified paper ballot. Id. Secretary Bradbury's conclusion that DREs lacking voter verified paper ballots do not provide the basis for a recount under state law applies with equal force to New Jersey's statutory law, and should be adopted by this Court. Paperless DREs function in direct opposition to the spirit and letter of New Jersey law concerning recounts.

B. In The Event Of A Recount, DRE Voters Have No Assurance That Their Votes Will Be Treated The Same As Votes Cast On Paper Ballots, Ballot Cards Or Lever Machines. This Unequal Consideration Of Votes Violates The Right To Equal Protection Guaranteed By The New Jersey Constitution.

[69] Available at http://www.sos.state.or.us/executive/speeches/110603op.htm (November 6, 2003).

The mere fact that specific guidelines exist in Title 19 for recounting votes cast on paper ballots, ballot cards and lever machines, but not for votes cast on DREs, simply denies DRE voters the right to equal protection guaranteed by the New Jersey Constitution.

Votes cast on DREs scheduled for use in the November election do not produce tangible evidence of voter intent, and therefore cannot be "recounted" like paper ballots, ballot cards or the observable movements of a lever-based voting machine. This means that, in the event of a recount, the votes of those who do not vote on DREs, who make up a minority of voters, will determine the outcome of the election, as those are the only votes that can be verified independently.

Atlantic, Bergen, Burlington, Gloucester, Hudson, Hunterdon, Mercer, Middlesex, Morris, Ocean, Passaic, Salem, Somerset, Sussex, and Union counties have purchased DREs. NJ Voting Equipment Inventory as of March 2004.[70] As of June 2004, approximately 3.3 million registered voters lived in those counties. New Jersey Division of Elections, Registered Voters as of the Close of Registration for the Primary Election to Be Held on June 8, 2004.[71] This year's successful "get-out-the-vote" efforts have undoubtedly swelled that number. See, e.g., Cowen, Voter Registration Crush in N.J.; Many Beat Deadline, Citing Presidential Race, at A01; Larini,

---

[70] At http://www.njelections.org/voting_machine_co_listdoe.html.

[71] At http://www.state.nj.us/lps/elections/6-04-by-county.pdf.

Signing to Vote in Nick of Time - N.J. Sees Landslide of Last-Day Registrations, at 1; Zernike, As Deadlines Hit, Rolls of Voters Show Big Surge, at A1.

Should the 2004 Presidential vote in New Jersey require a recount, counties using DREs will have no option but to rely on printed summaries of encoded data from machines that are prone to manipulation and error. DRE voters have no firm assurance that their votes will be actually recorded and recounted. Indeed, there are no guidelines whatsoever to guide county officials in performing a recount where DREs have been used.

In sharp contrast, all New Jersey citizens who vote by absentee, emergency, or provisional ballot are guaranteed to have their votes counted in the event of a recount, even if they reside in the fifteen counties that are using DREs. Moreover, all voters in the counties currently using lever machines or optical scanning machines will be certain that their votes are counted (and their voices heard) in a recount.

As of June 8, 2004, there were approximately 1,206,412 registered voters in the five counties (Camden, Cape May, Cumberland, Essex, Monmouth, according to the NJ Voting Equipment Inventory as of March 2004) who will be using lever machines, and 58,127 registered voters in Warren County, who will be using an optical-scan system. New Jersey Division of Elections, Registered Voters as of the Close of Registration for the Primary Election to Be Held on June 8, 2004. There are at least 3,359,465 registered voters in the fifteen counties scheduled to use DREs on Election

Day. Id.; NJ Voting Equipment Inventory as of March 2004. Thus, for every four New Jersey residents whose votes are guaranteed to be counted in the event of a recount, there are approximately eleven whose votes cannot be verified.

In the event of a recount, votes cast by paper or by lever machine will receive undue weight simply because they are the only votes that can truly be recounted. If the margin of victory in this presidential election is as close as it was in 2000, extra weight given the "recountable" votes could affect the outcome of the contest.

This unequal treatment of voters in the event of a recount violates the right to equal protection guaranteed by the New Jersey Constitution. Article 1, Paragraph 1 of the New Jersey Constitution protects against "the unequal treatment of those who should be treated alike." Greenberg v. Kimmelman, 99 N.J. 552, 568 (1985). In comparison to Fourteenth Amendment guarantees, "our State Constitutions have been construed to provide analogous or superior protections to our citizens." Peper v. Princeton Univ. Board of Trustees, 77 N.J. 55, 79 (1978).

In analyzing equal protection challenges, New Jersey courts have rejected the rigid approach followed by the federal courts. Instead, New Jersey courts rely on a flexible three-part balancing test to determine whether an action violates equal protection. Barone v. Dep't of Human Services, 107 N.J. 355, 368 (1987),(quoting Borough of Collingswood v. Ringgold, 66 N.J. 350, 370 (1975), appeal dismissed, 426 U.S. 901 (1976)). The test

examines "the nature of the affected right, the extent to which the governmental restriction intrudes upon it, and the public need for the restriction." Greenberg, 99 N.J. at 567. New Jersey's equal protection analysis requires "a real and substantial relationship between the classification and the governmental purpose which it purportedly serves." Taxpayers Ass'n of Weymouth Township v. Weymouth Township, 80 N.J. 6, 55 (1976).

In the event of a recount, the equal protection rights of DRE voters will be violated. Here, the nature of the voters' affected right, to have their votes counted, is of the highest magnitude. The right to vote is constitutional and fundamental. "A citizen's constitutional right to vote for the candidate of his or her choice necessarily includes the corollary right to have that vote counted '"at full value without dilution or discount."'" Gray-Sadler, 164 N.J. at 474 (quoting Reynolds, 377 U.S. at 555 n.29 (quoting South v. Peters, 339 U.S. at 279 (Douglas, J., dissenting))).

The second Greenberg factor is the extent to which use of DREs intrudes upon the affected right. In the case of a recount, the intrusion is total. As discussed at length above, the right to have election officials publicly examine the votes cast cannot be honored where there is no observable physical product of the voting process, but merely a reiteration of a biased technician's conclusion. Non-DRE voters enjoy the security of knowing their votes will be examined and confirmed in a recount. DRE voters do not.

The final Greenberg factor concerns the public need the restriction addresses. The focus is "whether there is an appropriate governmental interest suitably furthered by the differential treatment" embodied in the complained-of action. Barone, 107 N.J. at 368 (quoting Ringgold, 66 N.J. at 370). There is no public benefit in recording votes on an insecure system that provides no independent audit of votes.

Voting systems that do not generate a physical product that indicates voter intent cannot recount votes in a manner consistent with the spirit and letter of New Jersey election law. In the event of a recount, fraud or error in the computation of DRE vote totals cannot be detected, and the true intent of the voters cannot be confirmed. The inability to confirm the intent of DRE voters in a recount exposes those voters to a significant risk of disenfranchisement not shared by other voters. This inequality concerning the protection of a fundamental right violates the equal-protection rights of DRE voters under the New Jersey Constitution.[72]

III. ELECTRONIC VOTING MACHINES ARE TOO INSECURE TO PROTECT THE STATUTORY RIGHTS OF VOTERS.

New Jersey, in order to protect its residents' right to vote, has passed stringent statutory requirements that all voting

[72] Plaintiffs do not assert a federal constitutional claim, but note that Bush v. Gore, 531 U.S. 98, 109 (2000) established that inconsistencies in recounting can violate citizens' Equal Protection rights as guaranteed by the Fourteenth Amendment of the United States Constitution.

machines must meet. Machines, electronic or manual, which do not satisfy these requirements, deny New Jersey voters their right to choose their government. The Sequoia Voting Systems and ES&S electronic voting machines New Jersey counties intend to use on Election Day have extensive histories of malfunctioning nationwide, and are highly vulnerable to external tampering.

The Governor and Attorney General have not taken any measures to secure the electronic voting machines (as was done in California, Maryland, Nevada, and Ohio). Although it is impossible to predict that the machines will malfunction on Election Day, this Court should nonetheless intervene. The risk that voters will be disenfranchised by insecure voting machines that do not meet the statutory requirements outlined in N.J.S.A. 19:48 et seq. and 19:53A et seq. is simply too great.

In the past, DREs of the exact make and model to be used in New Jersey have attributed votes for one candidate to another, or simply failed to record votes. The instances of DRE malfunctions detailed above in other elections demonstrate that DREs are simply too unreliable to "be used safely, efficiently, and accurately in the conduct of elections and counting ballots," as mandated by N.J.S.A. 19:53A-3(g).

These requirements all assume, and are in conjunction with, the requirement that machines have been tested and certified. As detailed above, the process for certifying machines under N.J.S.A. § 19:48-2 does nothing to ensure that DREs will record and count votes accurately. Because the DREs which are scheduled to be used

on Election Day cannot be reliably tested under current New Jersey law, they fail to meet the further statutory requirements mandated by N.J.S.A. §§ 19:48-1, 19:53A.

A. DREs Prevent Voters From Casting Ballots, In Violation Of New Jersey Law.

Voting machines, both electronic and manual, are required by New Jersey law to allow voters to cast their ballots for the candidate(s) of their choosing, and to vote for or against any issue currently on the ballot. N.J.S.A. 19:48-1(d),(f); 19:53A-3(b) (2004). Electronic voting machines such as those scheduled for use in fifteen counties on November 2, 2004 have denied voters this right in other states' elections.

Sequoia Pacific AVC Edge machines in Boca Raton, Florida repeatedly registered the votes for the frontrunner as having been cast for his opponent. The opponent was declared the winner. Olson, Out of Touch. As discussed earlier, Salem County has purchased 160 of these machines. Over 40,000 registered voters are scheduled to use the AVC Edge machine on Election Day.

Machines manufactured by ES&S have similarly denied voters the right to choose their candidate. Voters in Texas in 1998 reported that votes cast for Democratic candidates registered as votes for their opponents. Gary Ashwill & Chris Kromm, Who Counts the Votes?, Southern Exposure, Winter 2002/2003.[73] As discussed above,

[73] Available at http://www.southernstudies.org/reports/votingmachines-new.htm (last visited Oct. 14, 2004).

more than 82,000 registered voters are scheduled to use ES&S iVotronic machines in Sussex County on Election Day.

Either intentionally or mistakenly, electronic voting machines are likely to not "[p]ermit each voter to vote . . . for all persons and offices for whom and for which he is lawfully entitled to vote." N.J.S.A. 19:53A-3(b); see also N.J.S.A. 19:48-1(d), (f). As Professor Appel noted, "faulty software could very easily add a number to the wrong total when a vote is cast, or make some other error, thereby misrecording a vote." Appel Certif. 12.

B. DREs Have Repeatedly Failed To Meet The Security Design Requirements Under New Jersey Law.

Electronic voting machines are further required by New Jersey law to "[b]e suitably designed . . . [to] be used safely, efficiently, and accurately in the conduct of elections and counting ballots." N.J.S.A. 53A-3(g). Design flaws on DREs of the type scheduled for use in New Jersey on Election Day leave the machines highly vulnerable to tampering.

As discussed above, the DREs scheduled to be used in New Jersey on Election Day are not suitable designed to count votes accurately. All DREs to be used can be readily tampered with to manipulate election results and throw elections.

Due to a lack of "transparency," manipulation of DREs is likely to go undetected. Appel Certif. 18-28; Mercuri Certif. 9. Fraudulent DRE software may appear legitimate when in fact it is a malicious. Appel Certif. 55, 70. Malicious DRE software can run a self-test and tell the testing agents exactly what they

want to hear, while silently manipulating votes. Id. Fraudulent software can provide a real-time clock that is read by the software that instructs the program to act properly on any day except Election Day, when it will manipulate votes. Appel Certif. 19.

Moreover, there are deficiencies in the physical design of the DREs that run afoul of N.J.S.A. 19:53A-3(g). The examples given below are a small sampling of the vulnerabilities of DREs discussed in great detail above.

Both the Sequoia Pacific AVC Advantage and AVC Edge have a reset button on the outside of the machine that allows a poll worker to (intentionally or unintentionally) permit a voter to cast more than one vote. Mercuri Certif. 23. The software in the AVC Advantage can be overhauled in just ten minutes by replacing a small chip. Appel Certif. 53. The software in the AVC Edge can be completely overridden in just five minutes by removing a cartridge on the side of the machine. Id. at 50. Unauthorized users can easily access unencrypted data stored on the AVC Edge memory card, including voting results. Mercuri Certif. 28,50. The ES&S iVotronic's software can be completely overridden in a matter of minutes. Compuware at 141.

The security deficiencies outlined above have become well-known. Thus, there is a risk that the electronic voting machines could be tampered with on Election Day, either remotely or at polling and tabulation sites by someone who has physical access to the DRE. Vote counts could be altered, affecting which candidates are elected.

C. DREs Such As Those Purchased in New Jersey Have Extensive Histories of Erroneously Reporting Election Results, In Violation Of New Jersey Law.

Manual and electronic voting machines must record and "accurately" count all votes cast. N.J.S.A. 19:48-1(h), 19:53A-3(h). The instances of DRE malfunctions across the United States demonstrate that DREs frequently fail to accurately votes. The risk is high they will do so in the fifteen counties which have purchased DREs.

Sequoia Pacific AVC Edge machines have purged votes originally recorded. Ackerman, Electronic Voting's Hidden Perils; Zoretich, Election Results Certified After Software Blamed, at A2. ES&S iVotronic machines failed to count votes, sometimes thousands of them. Haggman, When Did She Know, at 1.

As discussed above, over 40,000 registered voters are scheduled to vote on 160 Sequoia Pacific AVC Edge machines in Salem County on Election Day. In Sussex County, at least 82,000 registered voters in Sussex County are scheduled to use ES&S iVotronic machines.

IV. PLAINTIFFS ARE ENTITLED TO PROVISIONAL INJUNCTIVE RELIEF.

The standard for granting temporary injunctive relief pending the outcome of litigation is well settled. Crowe v. De Gioia, 90 N.J. 126, 132 (1982); N.J. State Bar Ass'n v. N. N.J. Mortgage Assoc., 22 N.J. 184, 193 (1956). Where there is a substantial

likelihood that plaintiffs will ultimately prevail on the merits, they should be granted provisional relief "where the injury to the moving party will be irreparable if the relief is denied, and where the inconvenience or loss to the opposing party will be minimal if the relief is obtained." Suenram v. Soc. of Valley Hosp., 155 N.J. Super. 593, 597 (L. Div. 1977).

In the instant case, Plaintiffs more than satisfy the required standard. Accordingly, Plaintiffs respectfully request that this Court enjoin the use of DREs and order that only paper ballots be used on Election Day. It should require that every citizen who wishes to vote, vote by emergency paper ballot, as described in N.J.S.A. 19:53B-1, or by absentee ballot, as described in N.J.S.A. § 19:57-1, and that these ballots will be tabulated by optical scan. This Court should also order that all existing DREs in New Jersey be retrofitted with voter verified paper ballots for use in future elections.

A. Denial Of The Requested Injunction Would Cause Irreparable Harm To Plaintiffs.

The irreparable harm that will fall upon Plaintiffs if the injunctive relief is denied far outweighs any inconvenience or expenditure the Defendants may experience or incur. New Jersey's Supreme Court has observed that "[h]arm is generally considered irreparable in equity if it cannot be redressed adequately by monetary damages." Crowe, 90 N.J. at 132-33. This is most certainly the case here. No amount of money can replace the

disenfranchisement of qualified voters should DREs malfunction or be manipulated to alter election results.

The right to vote is enshrined in the New Jersey Constitution, and has been recognized as fundamental by the Supreme Courts of New Jersey and the United States. Because it is so fundamental, and so strongly protected by New Jersey and federal law, this Court should take immediate action to ensure that every vote will be counted on Election Day.

It is impossible to predict whether or not any DREs scheduled for use will malfunction or be manipulated on Election Day. But one reason we cannot predict this is because the voting systems of DREs are inherently flawed. The software that instructs the computer how to count votes is secret. Waiting until Election Day to see which under-tested voting machine will fail to perform is too great a risk to take. The machines have extensive histories of malfunctioning across the nation, both while being tested and during actual elections. When the machines malfunctioned, they failed to count votes. As discussed above, the loss of even one vote is anathema to New Jersey Constitutional and New Jersey statutory law.

Because of the severity of the constitutional deprivation which would occur from malfunctioning or manipulated electronic voting machines, this Court should enjoin the use of all DREs in the upcoming election.

B. Any Inconvenience Or Loss Defendants May Experience Is Minimal, When Compared To Plaintiffs' Loss.

The Defendants will not be harmed if this Court enjoins the use of DREs for the November election. Both Governor McGreevey and Attorney General Harvey have a duty to enforce the laws of this State. They also have the authority to issue executive orders to ensure the DRE voting process does not disenfranchise any New Jersey voters.

Alternate methods for casting votes in New Jersey already exist and should be used on November 2, 2004. Given the nature of the relief involved, the cost of ordering the requested relief is minimal.

1. The Use of Emergency Ballots Should Be Available To All New Jersey Voters.

Requiring that votes be cast on paper ballots in each county simply extends processes already required by statute. N.J.S.A. § 19:53B-1. The preparation, use, counting and storage of emergency ballots is already provided for in Chapter 53B of New Jersey's Title 19. Because these ballots must already be printed, distributed, counted, and tallied, no real hardship exists in extending their use to all New Jersey voters.

The county clerk, or municipal clerk in a municipal election, is responsible for preparing an emergency ballot packet. See N.J.S.A. § 19:53B-1(a). The statute provides for physical specifications of the emergency ballots. N.J.S.A. § 19:53B-1(c).

Strict guidelines regulate the placement and distribution of emergency ballots. The emergency ballots are not to be distributed outside the polling room and the specific district. N.J.S.A. §

19:53B-2(a). No envelopes are to be kept in areas where voters mark their ballots. N.J.S.A. § 19:53B-2(b). Sufficient pencils are to be provided for the voters to mark their choices. N.J.S.A. § 19:53B-2(c). Each county's Board of Elections is to prepare written instructions for the procedures each District Board Members is to carry out. The Members are orally instructed on these procedures at the district's training classes. Id.

Each district election must have a supply of emergency ballots, provided at the polls. N.J.S.A. § 19:53B-3(a) (2004). The mode and manner of voting shall still follow the statutory guidelines as closely as possible. Id.

If no emergency ballots are ready or available, or if the supply has run out before the polls close, the chief District Board Member shall notify the appropriate authority that additional emergency ballots are required. N.J.S.A. § 19:53B-3(b). The statute mandates the symbols with which a voter can mark his/her choice for each office on the ballot, N.J.S.A. § 19:53B-7, and the manner in which a vote may be case for a write-in candidate on an emergency ballot. N.J.S.A. § 19:53B-8.

Provisions also exist for the placement, deposit, canvassing, reading, tallying, and storage of emergency ballots and the emergency ballot box. N.J.S.A. §§ 19:53B-4 to -5, -10 to -11, -13, -17 to -20.

Guidelines for every conceivable occurrence relating to emergency ballots are detailed in the statute. These provisions include: the rules for challenging a voter's right to vote,

N.J.S.A. § 19:53B-12 (2004); the requirement for voting secrecy and the consequences of a violation of this secrecy, N.J.S.A. 19:53B-6 (2004); the procedures that shall be carried out in the case of a spoiled, invalid or void emergency ballot. N.J.S.A. §§ 19:53B-9, -14 to -15 (2004); the finality of a decision made by the majority of a District Board over any question and the procedure for a Member's dissension from that decision. N.J.S.A. § 19:53B-16 (2004).

Because these statutory provisions have been in place since 1992, and provide for all printing, distribution, tallying, and storage of emergency ballots, as well as all imaginable contingencies that could arise, the State of New Jersey and its election officials will be able to accommodate a state-wide emergency ballot vote without hardship.

2. The Statutory Provisions For Optical Scan Tabulation of Absentee Ballots Should Be Applied In Order To Efficiently Count Court-Ordered Emergency Ballots.

The challenge presented in ordering the use of emergency ballots is that no statutory provision exists for electronic, optical, or mechanical counting of the ballots. They must be counted by hand. N.J.S.A. 53B-18.

Admittedly, processing each voter's cast ballot by hand is not the most efficient method to count votes. Fourteen of the fifteen counties that use DREs, however, use optical scanning methods to process their absentee ballots. They therefore have machines

available to tally ballots faster than if the tally were done by hand.[74]

The Court should order that the emergency ballots to be used by voters on November 2, 2004 be formatted to be counted by the optical scanning method described in N.J.S.A. § 19:57-15.1 (2004), governing the counting of absentee ballots. This statute provides for the tallying of absentee ballots by any "system of electronic scanning, other mechanical or electronic device . . . previously approved by the Secretary of State . . ." Id. Additionally, the statute allows

> [t]he county clerk in any county adopting such a system [to] prepare and use absentee ballots that do not conform generally to the ballot to be used at said election to the extent that such nonconformance is necessary in the operation of the electronic or mechanical canvassing system.

Id.

Professor Appel states in his Expert Report, Mercer County officials could process 1,000 scanned votes in ten minutes. Appel. Certif. 71. There are 189,717 registered voters in Mercer County as of March 2004. Assuming that all the voters vote via absentee ballot, it would take just under three hours and ten minutes to scan all of the votes. The relative cost of this method of voting is negligible when compared to the cost of disenfranchising voters.

---

[74] Office of the Attorney Gen., N.J. Dep't of Law and Pub. Safety, NJ Voting Equipment Inventory as of March 2004.

It is within this Court's equitable power to order the most efficient method of tabulating paper ballots in this special circumstance. "'Courts of equity may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to go when only private interests are involved.'" Texas Co. v. Di Gaetamo, 71 N.J. Super. 413, 430 (App. Div. 1962) (quoting Mercoid Corp. v. Mid-Continent Inv. Co., 320 U.S. 661, 670 (1944) (internal quotations omitted)). Thus, this Court should order that the emergency ballots produced for the election be formatted with a scanning device so that they can be optically scanned, rather than counted by hand.

C. New Jersey Courts Have Not Shied Away From Ordering Special Relief When The Right To VOte Has Been Compromised By Voting Machine Malfunctions.

Enjoining the use of DREs this Election Day would be in keeping with New Jersey law. The New Jersey judiciary has a long and honorable record of taking every necessary step to ensure every vote is counted. New Jersey courts have consistently set aside elections where there is evidence of tainted results caused by malfunctioning voting machines. When machines fail to work properly and capture votes, such action is necessary to protect New Jersey voters' constitutionally-protected rights.

> When dealing with the malfunction of a machine which affects the will of a substantial number of voters, the election takes on the aura of uncertainty and unfairness calling

> for judicial intervention. And if the evidence supports a finding that sufficient numbers were prevented from voting for reasons beyond their control so as to create the potential of a different result, the election should be set aside.

In Re Petition of Hartnett, 163 N.J. Super. 257, 268 (App. Div. 1978).

In Re the Application of Moffat concerned a voting machine malfunction, which caused a recording mechanism within the machine to become dislodged. 142 N.J. Super. 217, 222 (App. Div. 1976). The broken machine did not count any votes for the petitioner after the first vote was cast. Id. The trial judge concluded that many votes were not counted. Id. The Appellate Division affirmed and set the election aside since the voting machine malfunction made it impossible to ascertain who the true winner of the election was. Id. at 226. Further, the court held that it is not necessary to prove who would have received the uncounted votes before setting aside the election. To set aside an election, a candidate need only show that enough votes were set aside so as to effect the outcome of the election. Id. at 225-26.

New Jersey courts' willingness to set aside elections where voting machines malfunctioned is further demonstrated in In Re the 1984 General Election for the Office of Council of the Township of Maple Shade, 203 N.J. Super 563 (L. Div. 1985). In Township of

Maple Shade, numerous voters were turned away from the polls after a single voting machine broke. Id. at 570. During the three and a half hours in which the machine was not working, at least 14 voters left the polls without voting. Id. Despite the fact that alternative methods such as emergency ballots were available for voters to use, the election was still set aside by the judge as these measures were not properly implemented. Id. at 590.

New Jersey courts will typically set aside elections where there is evidence that legal votes were rejected and not accurately counted. The court in Magura v. Smith interpreted the term "rejected" to include "any situation in which qualified voters are denied access to the polls including a denial because of shutdown of a voting machine." 131 N.J. Super. 395, 399 (L. Div. 1974). Thus, New Jersey courts are likely to set aside elections if DRE malfunctions that already occurred elsewhere occur in New Jersey.

Hartnett and Moffat demonstrate the great lengths the New Jersey judiciary has taken to ensure that every vote is counted. Given its broad mandate to uphold the Constitution and laws of New Jersey, this Court is empowered to take immediate action to enjoin the use of DREs on Election Day, thus averting serious harm to New Jersey voters. Such action would be identical to actions taken by the Supreme Court of Venezuela, the Secretaries of State of

California, Nevada, and Ohio, and the Republic of Ireland, all of which declared that DREs are simply too insecure to use in their elections.

As the study at Yale University demonstrated, the loss or alteration of a single vote on each machine could affect the outcome of an election. DiFranco et al., Small Vote Manipulations Can Swing Elections, at 44-45. Thus, undetectable manipulations can severely impact an election.

Electronic voting machines in New Jersey contain no mechanism to ensure a verified recount in the event of a contested election result. There is a very serious risk that if no action is taken, the will of New Jersey voters will be denied due to the loss of substantial numbers of votes. In the event of a recount, only a minority of the votes cast are guaranteed to be counted, and will determine the election. It would be impossible to determine if that minority sample accurately reflects the will of the majority. The immediate relief Plaintiffs seek is the only way to ensure such a debacle does not occur. This Court should intervene now, before serious malfunctions occur that will jeopardize the integrity of the election.

CONCLUSION

For the reasons stated herein, this Court should enjoin the use of DREs for the upcoming November 2004 election. It should order that all votes be cast on paper ballots. It should further enjoin the use of all DREs in New Jersey until the Office of the Attorney General enacts guidelines for their use and updates the statutory provisions governing their certification. To address the inherent security risks of DREs that remain once action is taken, this Court should order that all DREs purchased by New Jersey counties be retrofitted to provide a voter verified paper trail after the November 2004 election. Finally, this Court should require that all new DREs purchased in the State require a voter verified paper ballot.

Only if this proposed action is taken can this Court ensure that Plaintiffs' and other New Jersey citizens' fundamental right to vote will be preserved.

Respectfully submitted,

_____
Penny M. Venetis
Constitutional Litigation Clinic
Rutgers School of Law - Newark
123 Washington Street
Newark, NJ 07102
(973) 353-5687

Counsel for the Plaintiffs

October 19, 2004