ANNE MILGRAM
ATTORNEY GENERAL OF NEW JERSEY
Richard J. Hughes Justice Complex
·25 Market Street
PO Box 112
Trenton, NJ 08625-0112

By: Leslie Gore
Deputy Attorney General
(609) 984-1063

	SUPERIOR COURT OF NEW JERSEY LAW DIVISION - MERCER COUNTY DOCKET NO. MER-L-2691-04

Formatted Table

ASSEMBLYMAN REED GUSCIORA, STEPHANIE HARRIS, COALITION FOR PEACE ACTION, and NEW JERSEY PEACE ASSOCIATION, Plaintiffs, v. JON S. CORZINE, Governor of the State of New Jersey (in his official capacity) and ANNE MILGRAM, Attorney General of the State of New Jersey (in her official capacity), Defendants.	: : : : : : : : : :	Civil Action REBUTTAL REPORT OF MICHAEL I. SHAMOS

BACKGROUND & QUALIFICATIONS

1. My name is Michael I. Shamos. I hold the title of Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. I was a founder and Co-Director of the Institute for eCommerce at Carnegie Mellon and I now direct a graduate degree program in eBusiness Technologies. My résumé is attached as Exhibit 1 to this report.

2. I teach graduate courses at Carnegie Mellon in Electronic Commerce, including eCommerce Technology, Electronic Payment Systems, Electronic Voting and eCommerce Law and Regulation and have done so since 1999. In fall 2007 I am teaching Law of Computer Technology.

3. From 1979-1987 I was the founder and president of two computer software development companies in Pittsburgh, Pennsylvania, Unilogic, Ltd. and Lexeme Corporation.

4. I am an attorney admitted to practice in Pennsylvania and have been admitted to the Bar of the U.S. Patent and Trademark Office since 1981.

5. From 1980 through 2000 I was a statutory examiner of computerized voting systems for the Commonwealth of Pennsylvania. During that period, I participated in every electronic voting system certification examination conducted in Pennsylvania.

6. From 2005 to the present I have again served as statutory examiner of computerized voting systems for the Commonwealth of Pennsylvania pursuant to the Pennsylvania Election Code, 25 P.S. §3031.5.

7. From 1987-2000 I served as statutory designee of the Attorney General of Texas for examination of voting systems pursuant to the Texas Election Code. During that period, I participated in every electronic voting system certification examination conducted in Texas.

8. I have examined voting systems for the duly constituted authorities in Massachusetts (2006), Delaware (1989), Nevada (1995) and West Virginia (1982). To date I have performed over 120 electronic voting system certification examinations.

9. All of the reports of my examinations in Pennsylvania and Texas are public records maintained by the Secretary of the Commonwealth of Pennsylvania and the Secretary of State of Texas. All of my examinations in Pennsylvania have been recorded on video, copies of which are maintained by the Secretary of the Commonwealth.

10. I have been invited to speak on electronic voting at conferences and panels by the League of Women Voters, the County Commissioners Association of Pennsylvania, the Election Center, John Marshall Law School, Ohio State Moritz School of Law, University of Maryland, Pace University, University of Hong Kong, International Workshop on Mathematics and Democracy, Rutgers University, National Institute of Standards and Technology, American Association for the Advancement of Science, Congressional Black Caucus, Election Assistance Commission, American Enterprise Institute and the U.S. Commission on Civil Rights.

11. I testified four times before committees of the U.S House of Representatives on electronic voting and once before the U.S. Senate Committee on Rules and Administration.

12. I have testified on electronic voting before the legislatures of Maryland, Pennsylvania, and Texas and the State Board of Elections of Virginia.

13. I am the sole author of three papers on electronic voting.

14. I am the author of a book manuscript entitled "A Glossary of Electronic Voting," which contains over 1000 definitions of terms relating to that subject.

15. I have previously testified in a number of cases concerning electronic voting. My résumé in Exhibit 1 contains a list of cases in which I have testified in the last ten years.

16. I have been retained as an expert by Attorney General of New Jersey, counsel for Defendants.

17. I have been engaged through Expert Engagements LLC ("EE"), a firm that locates expert services for law firms. EE charges $525 per hour for my services, of which I receive $475. I am one of the owners of EE. No part of my compensation is dependent on the outcome of this case.

18. I have been asked by counsel for Defendants to review and respond to the Expert Report of Andrew Appel, dated August 29, 2008 (the "Appel Report" or the "Report") and the attachments thereto.

19. It may be necessary for me to revise or supplement this report based on material subsequently presented by Plaintiffs, and I reserve the right to do so. I may also present demonstrative evidence at trial, and I reserve the right to do so.

20. It may be necessary for me to revise or supplement this report, or file a supplemental or responsive report, based on any responsive submission of Plaintiff, and I reserve the right to do so.

21. My failure here to specifically rebut or comment on a statement in the Appel Report does not necessarily mean that I necessarily agree with the statement.

SUMMARY OF OPINIONS

22. The Appel Report is a lengthy diatribe against electronic voting based on a litany of deficiencies in the system under review located by Dr. Appel and his colleagues after extensive experimentation under laboratory conditions. No comparable review was conducted of the very system Dr. Appel proposes as a replacement, namely an unspecified and unidentified optical scan system. Therefore, there is no scientific basis to suppose that any unexamined replacement system would be superior in any respect to the system reviewed.

23. The Appel Report does not even purport to articulate any standard by which the security of a voting system can or should be judged. Therefore its conclusion that "The AVC Advantage is too insecure to use in New Jersey" (p. 144) is not supported by any of the observations described in the Report. No bright line is given by which it could be determined whether a system is "too insecure," or what level of insecurity might be tolerable. Furthermore, Dr. Appel has conducted no evaluation whatsoever, of security or any other aspect, of any system he suggests New Jersey ought to adopt in place of the AVC Advantage.

24. Because no evaluation was conducted of any precinct-count optical scan system, there is no basis in the Report for Dr. Appel's conclusion that "New Jersey should immediately

implement the 2005 law passed by the Legislature, requiring an individual voter-verified record of each vote cast, by adopting precinct-count optical-scan voting equipment" (p. 144). The statute cited does not contemplate, or even appear to permit, optical scan voting in New Jersey.

25. The appropriate response to the discovery of security vulnerabilities is to remediate them, not to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure or whose security properties are unknown.

THE APPEL REPORT

26. The Appel Report (p. 1) claims to evaluate "the security and accuracy of the Sequoia AVC Advantage DRE voting computer" (the "System"). It does not constitute an evaluation of the security of the System under actual conditions of use in New Jersey. Furthermore, the methodology used to evaluate the "accuracy" of the System does not even minimally comport with the standards and methodology used in the trade or as promulgated by the Election Assistance Commission ("EAC") or statute for evaluating the accuracy of voting systems.

27. Paragraph 1.6 of the Report on p. 9 offers various opinions concerning the AVC Advantage. I do not agree that the processes described therein are practical to perform in a realistic election setting. However, I observe the following:

a. The "hack" described in ¶1.6.1 can be performed on DRE machines with VVPAT as well as optical scanners. In 2005, Harri Hursti, one of Dr. Appel's colleagues in the Report identified on p. 7, discovered a hack that can be used to steal votes on optical scanners. This exploit is described in "SECURITY ALERT: July 4, 2005 Critical Security Issues with Diebold Optical Scan Design[1]. This hack "can be perpetrated by a person with only ordinary training in computer science," as Dr. Appel claims of the Advantage hack in ¶1.6.2.

b. Assuming that "a person can easily gain enough access to voting machines to install this hack," as claimed of the Advantage hack in ¶1.6.3, the same is true of the Hursti hack on optical scanners.

[1] Available at http://www.blackboxvoting.org/BBVreport.pdf.

c. The opinion offered in ¶1.6.4 that the Advantage hack, once installed "is practically impossible to detect," is palpably incorrect. In the video accompanying his Report, Dr. Appel demonstrates how to detect it. Otherwise, he would not even be able to demonstrate its existence. Furthermore, this hack would immediately be revealed by the simple expedient of parallel testing, described later in this rebuttal.

d. The opinion in ¶1.6.5 that "once installed on a voting machine, the fraudulent firmware can steal votes in election after election without any additional effort," is incorrect. While it might be true if no tests or examinations were performed on the voting machine, and if no firmware updates are installed, but this is not the case in practice. Even if true, however, it is equally applicable to DREs with VVPATs and optical scanners.

e. The opinion in ¶1.6.6 that "the AVC Advantage is vulnerable to hacks (fraudulent manipulation) in several different ways," is equally true of DREs with VVPATs and optical scanners.

f. The opinion in ¶1.6.7 that "some of these hacks take the form of viruses that can automatically propagate themselves from one voting machine to another" is not supported by any experiment or examination described in the Report. Even if true, it is likewise true of DREs with VVPATs and optical scanners.

g. The opinion in ¶1.6.8 that "even when not 'hacked,' the AVC Advantage (in its normal state) has design flaws that can cause votes to be lost, or cause voters to be given the wrong primary ballot" is likewise true of DREs with VVPATs and optical scanners.

h. The opinion in ¶1.6.9 that "even when not 'hacked,' the AVC Advantage in its normal state has design flaws that encourage voter error and pollworker error, and permit fraud, even of true, is likewise true of DREs with VVPATs and is overwhelmingly true of optical scan systems.

28. Paragraphs 2.1-2.9 of the Appel Report purport to be an accurate description of the operation of the AVC Advantage. Unfortunately, Dr. Appel has embellished what should have been a factual presentation with unjustified editorial comments that render his statements incorrect.

29. For example, ¶2.1 states that "the computer stores data in its memory that (are supposed to) correspond to the indicated votes; and at the close of polls, the computer outputs (what are supposed to be) the number of votes for each candidate." The parenthetical phrases are unjustified by any observation made by Dr. Appel. The machine is not only supposed to do these things – it actually does them.

30. Paragraph 2.3 states, "Since there is no inherent internal connection between the buttons and the totals kept in memory and reported at the end of the election, erroneous or malfeasant software can readily add to the wrong total or make some other error at any time during an election, thereby misrecording votes." The conclusion does not follow from the premise. There is no voting system in existence in which there is an inherent connection between buttons and counters. Even mechanical lever machines possess no inherent connection between levers and counters. The connection is mediated by rods and gears, which may break or fail. I also challenge the use of the word "readily" to describe the behavior of erroneous or malfeasant software. First, erroneous software is easily detected by testing. Malware that attempts to disguise its presence is also detectable by a different sort of testing. The notion that these types of software can "readily" perform any function at all or that they can even be introduced into voting systems completely ignores administrative controls designed to prevent such occurrences.

31. Paragraph 2.3 states, "Even though the software produces a so-called audit trail' of the results, it can always display an 'audit trail' consistent with its fraudulent results, and report that it has performed correctly." This behavior was never observed by Dr. Appel, and he does not ever claim that it occurred. The AVC Advantage as certified does produce an audit trail (not a so-called one) that accurately captures every vote cast. What Dr. Appel is referring to is that a machine that has been altered fraudulently can produce a fraudulent audit trail, but the same is true of every audit trail in existence. An embezzler who wishes to conceal his activities can make fraudulent entries in the books of a corporation to cover his tracks. All that means is that it

is important to ensure either that fraudulent entries cannot be made, or that they will be detected if made.

32. For example, Dr. Appel implies that optical scan balloting is self-auditing, because the ballots themselves are available after the election to be recounted. But this is not the case. If the ballots are altered, lost or substituted, they no longer constitute an audit trail. In fact, under Dr. Appel's definition, no voting system provides an audit trail, including the voting systems he proposes to replace the AVC Advantage.

33. Paragraph 2.4 states, "Every so-called 'audit trail' in the AVC Advantage, including all records of votes, can be modified at the discretion of the firmware." This implies that the firmware makes some sort of informed decision whether to alter votes. It does not. All mechanisms that produce audit trails, whether in elections or any other activity, must be tested to ensure that the audit function is operating properly. Once that is established, the firmware exercises no "discretion" at all.

34. Paragraph 2.6 asserts that no amount of auditing will detect any discrepancy if there is fraudulent firmware in the voting machine. This is untrue. Fraudulent firmware differs from the original firmware. This difference can be detected. While it may not be possible, after detection, to reconstruct the actual votes, the results from that machine can be voided. If no race is affected, then the election can be certified. If one or more races are affected, it may be necessary to revote. But the assertion that fraudulent firmware cannot be detected is flatly wrong.

35. The footnote to ¶2.6 further asserts that "a DRE cannot be effectively audited." This is also false. If the audit mechanism is working and the software and firmware have been verified to be identical to the versions certified, then the machine is completely auditable. It is always true, in any sort of audit, electoral or otherwise, that the audit entries must be made and recorded accurately. If false information is fed to an audit trail, it will not serve its intended function.

36. I note that all of Dr. Appel's complaints about auditing DREs, even if accurate, would also apply to DREs with VVPAT and optical scan systems.

37. The footnote to ¶2.6 ends with an incorrect argument that optical scan machines can be effectively audited. This is false, and its falsity is apparent in every election cycle in the United States. If the original ballots have been altered, lost or replaced, absolutely no audit is possible. In an optical scan system, there is only a single record of the voter's choices. If that original is no longer available, no audit can be performed.

38. Paragraph 2.7 states, "it is absolutely crucial that firmware should be correct in all circumstances, and the voting-machine firmware should be immune to tampering." These statements are untrue. It is quite possible for voting firmware and software to contain bugs that are not exercised in normal operation, or that do not cause vote totals to be altered. Such firmware, even in the presence of error, is still safe for use in elections. In fact, it is virtually certain that all voting firmware and software contains bugs, but these are generally benign. There is no requirement that any component of a voting system be absolutely immune to tampering. That would impose an unreasonable perfection standard that is not achievable in practice. The primary risk is that tampering, if it occurs, be detected so that tainted results are not used to determine a winner. Furthermore, optical scan systems are much more vulnerable to tampering than any DRE, so if Dr. Appel is correct that voting systems must be immune to tampering, then New Jersey will not be able to conduct any further elections regardless of what system it may adopt.

39. Paragraph 2.8 contains erroneous statements. Dr. Appel claims to have found that "it is easy to replace firmware in the AVC Advantage with fraudulent firmware that can undetectably steal votes and thus change the outcome of elections." He found no such thing. Under artificial conditions he was able to replace the firmware in an Advantage and then without attempting to detect that the firmware was fraudulent, he showed that it could steal votes. That is a very different thing from injecting fraudulent software into a real election and having it go undetected.

40. In any event, as described earlier, Harri Hursti was able to alter the outcome of an optical scan election with the same ease. Therefore, Dr, Appel's statements, even if they were true, do not support the conclusion that optical scan is any more secure or should be mandated by the Court.

41. Paragraph 2.8 also avers that "some kinds of fraudulent firmware can automatically virally propagate themselves from one AVC Advantage voting machine to another." That is a purely hypothetical statement, since such viral propagation was not achieved or demonstrated by Dr. Appel. However, even if the statement were true, it would also be true of DREs with VVPAT and optical scanners.

42. Part I of the Appel Report, beginning on p. is devoted to explaining that fraudulent firmware can steal votes. Such a statement is obviously true, and needs no demonstration. This issue is whether one can create such software that would effectively evade detection and introduce it into a number of machines sufficient to affect the outcome of an election.

43. On p. 14, Dr. Appel again avers that fraudulent vote-stealing programs can be made "practically undetectable." However, he asserts that he did not do this, but instead made his program detectable "just to demonstrate it." There is no support for the statement that such programs can be made undetectable, and Dr. Appel has neither done that nor explained how it might be done. There is therefore no basis for his opinion on this point, and he is incorrect because parallel testing will reveal the presence of fraudulent code.

44. In ¶2.11, Dr. Appel opines that "it is easy to gain access to AVC Advantage machines owned by New Jersey counties, in order to tamper with them." First, neither Dr. Appel nor any of his colleagues has ever gained access to an AVC Advantage machine owned by a New Jersey county, so his discussion here is entirely fictional. However, even if such access were possible, the responsible action would be to plug the loopholes by which an intruder might gain access, not to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure, as proposed by Dr. Appel.

45. In ¶2.11, Dr. Appel states that "the locks and seals on the AVC do not prevent this tampering." Even if true, the responsible action would be to improve the locks, seals and tamper-evident tape to reveal tampering reliably, not to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure, as proposed by Dr. Appel.

46. Paragraph 3.1 repeats the canard that "it is not difficult to replace the firmware on the AVC Advantage with fraudulent firmware that steals votes while leaving no detectable evidence." First, it is very difficult, and Dr. Appel has not demonstrated that it could be done under authentic election conditions, as opposed to a laboratory. Second, there is no support at all for the statement that no detectable evidence would be left. Third, the statement would also apply to DRE machines with VVPAT and optical scanners.

47. Paragraph 3.3 repeats the averment that fraudulent software can perform any number of misdeeds. This statement is obviously true, and need not be belabored. The proper question to be asked is whether such software can actually be created, whether it can be introduced surreptitiously into an election without being detected, and, even if installed, can it evade detection by parallel testing. The answer to the question is a resounding "no."

48. Even if the opinions expressed in 3.3 are correct, they also apply to DREs with VVPAT and optical scan systems.

49. Paragraph 3.4 asserts that the "means now in use in New Jersey" are insufficient to detect fraudulent software. Even if true, the appropriate response is to implement effective means, not to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure, as proposed by Dr. Appel.

50. The discussion in Section 4 on p. 16, relating to fraudulent software evading detection, is completely defeated by parallel testing.

51. The hiding methodology of 4.2, waiting until the 150th voter casts a vote, is easily defeated by the methods described in the section below entitled, "Defeating Malware."

52. In ¶4.5, Dr. Appel offers the excuse that he deliberately built a less sophisticated vote-stealing program so he could demonstrate it to the Court. He explains that "a real vote-

stealing program would be more clever and would be practically undetectable." There is no scientific basis for such a statement. There is no evidence that Dr. Appel has ever built such a program, that he has any idea how to create one and no evidence that it is even possible to build one at all. These opinions are without factual or technical basis. One can infer that if Dr. Appel knew how to create such a program he would have done so, if only to support his opinion. I take his failure to furnish such a program, or even explain how it might be created, as evidence that he has no idea how it might be done.

53. A program of the type described in ¶4.6 would immediately be detected by parallel testing.

54. The scenario in ¶4.7 is overly simplistic. The proposed manipulation cannot guarantee that "primary challengers never win." For one thing, the contestants in a primary may not involve an incumbent, so there is not necessarily any notion of a "challenger." The hack proposed by Dr. Appel, even if it could be mounted, might guarantee the election of precisely the candidate the hacker was trying to defeat.

55. In ¶4.8 Dr. Appel claims that "the voting machines are hackable in exactly the state in which Union County had configured them for the election." This statement is false. The state in which Union County configured them had them stored under secured conditions in Union County. It is no trick to tamper with a voting machine in one's own laboratory with no one watching. Dr. Appel has not demonstrated that any of his proffered manipulations could be performed undetectably in practice.

56. The scenario presented in ¶¶4.11-4.15 is easily defended against and is not a realistic attack. I agree that if fraudulent firmware can be installed in a voting machine, and the installation is not detected, incorrect results can be reported. The obvious solutions are (1) to prevent tampering with machines or make such tampering evident; or (2) to validate before the election that the firmware installed in the machine is the authorized firmware; or (3) perform parallel testing. The responsible solution is not, as Dr. Appel concludes, to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure. I note

that the very exploit performed by Dr. Appel, if feasible on the AVC Advantage, is also feasible on DRE machines with VVPAT and optical scanners.

57. The supposed vote-stealing mechanism of ¶4.14, in which the malware waits for the 20th vote to be cast before engaging in illicit behavior, is easily detected by parallel testing or validation of the firmware.

58. Any manipulation in which the intruder, as described in ¶4.15, can accomplish the instruction by defeating locks and seals, can also be defended against by strengthening the security of the locks and seals. The responsible solution is not, as Dr. Appel concludes, to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure.

59. I observe that the locks and seals on DRE machines with VVPAT, and particularly optical scanners, are not any more secure than those on the AVC Advantage. Therefore, Dr. Appel has no basis on which to conclude that the AVC Advantage is any less secure.

60. Section 5, deals with replacement of ROM chips in the AVC Advantage simply makes the obviously correct point that if one is able to gain access to a machine and transform it into a different machine by replacing components, then the transformed machine cannot be expected to perform the way the original did. There is no need to hire a computer scientist from Princeton (or even Carnegie Mellon) to so testify. The same proposition is true of every machine on Earth, whether it is a voting machine or not. The responsible solution is not, as Dr. Appel concludes, to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure. The response should be to (1) improve the physical security of voting machines; (2) improve the security of the locations in which voting machines are stored; and (3) perform firmware validation prior to each election. That solves the problem. I note that the very exploit performed by Dr. Appel, if feasible on the AVC Advantage, is also feasible on DRE machines with VVPAT and optical scanners.

61. I agree with the statement in ¶5.7 that plastic-strap seals provide only a veneer of tamper detection, and that an experienced intruder would easily be able to replace any such seal

he might break with an excellent forgery. However, that does not mean that such seals are useless, merely that they should not be relied upon as the sole intrusion detection mechanism.

62. Paragraph 5.8 is misleading – in my opinion, deliberately so – concerning the function of the checksum in the AVC Advantage. The purpose of a checksum is to detect errors. All computer memories can fail, and all do after a period of use. It may happen that the firmware contains a "1" bit in a particular location, but when the memory is read it erroneously outputs a "0." If the code were to execute with this error, incorrect results could be produced. Thus the ROM contains code to check whether such errors have occurred. Dr. Appel incorrectly states that the checksum is a security measure: "That is, it attempts to detect the replacement of itself! This is not an effective security measure, because once the firmware is replaced, obviously it is no longer there to perform this detection." (Report, ¶5.8.) This is a classic straw man argument. Dr. Appel wrongly asserts that the checksum is a security mechanism, shows that it is inadequate for that purpose, and on that basis criticizes the machine for poor security.

63. The error is repeated in ¶5.9, which states, "the design of the AVC Advantage's ROM-checksum algorithm is so weak and insecure that I was easily able to construct a fraudulent firmware with a checksum that matched the legitimate one." A person with Dr, Appel's experience in computer security knows that checksums are not intended to be used to detect intrusions, and are not in fact used that way.

64. The observation in ¶5.10 is similarly misleading. It is well known that the purpose of a Maintenance Log in a voting machine is not to detect malicious substitution of firmware, but to record various events in which a machine is involved. It is no criticism to observe that the Maintenance Log does not perform a function it was not intended to perform. I note that Dr. Appel's maintenance log complaint also applies to DREs with VVPAT and optical scanners.

65. Section 6 on p. 23 attempts to argue, incorrectly, that vote-stealing firmware can avoid detection. First, the scenario suggested by Dr, Appel is preposterous. He sets forth in paragraphs 6.3-6.10 a list of requirements that such firmware would have to satisfy. Some of

them cannot even be implemented in a laboratory, let alone a functioning voting machine, since no one on Earth, including Dr. Appel, knows how to do so.

66. For example, ¶6.5 requires that "the fraudulent firmware must take care not to steal too many votes." First, it is not known or generally agreed how many is too many. That certainly depends on the demographics of the jurisdiction, the nature and history of the race in question, and the behavior of the candidates as the election approaches. Even if the demographics were known, in what sort of database would it be hidden? After all, the races and demographics are different for each precinct in a county, and even a single city typically has thousands of precincts. Dr, Appel repeatedly states that his fraudulent firmware can remain in a machine and continues to operate in election after election. If that is so, where would it get the necessary time-varying information about demographics and the behavior of candidates? It can't.

67. Dr. Appel states incorrectly that "Experts in the field of election auditing usually assume that 20% of the votes can be stolen without raising suspicions." First, there are no experts in the field of election auditing. Second, Dr. Appel cites as authority for the 20% figure a white paper by Howard Stanislevic entitled "Random Auditing of E-Voting Systems: How Much is Enough?" This is not a scientific or scholarly paper. Its author is not a recognized expert or authority on voting systems, but is simply an outspoken advocate for VoteTrustUSA, an organization whose avowed agenda is the elimination of DRE voting in the United States. Even so, a minute reading of the complete text of the paper fails to reveal a single place in which it is even suggested that 20% of votes can be swapped without raising suspicions. Such a conclusion would not comport with everyday experience. Any discrepancy between poll results and election returns always raises suspicions, and the 20% figure, which would result in a swing of 40% (subtracting 20% from one candidate and adding 20% to another) would instantly provoke a claim of foul.

68. Paragraph 6.6 observes that the fraudulent firmware would have to behave properly during pre-LAT testing. That is obvious and has been known for decades. Such a scenario was

described in my early examiner's reports in Pennsylvania during the 1980s. The error is in believing that the purpose of pre-LAT is to detect malicious software. It isn't. The purpose of pre-LAT is to detect errors in ballot setup. It presupposes that the software and firmware are working properly and ensures that every candidate is on the electronic ballot and is associated with the correct party. No examiner relies on pre-LAT to verify the correctness of software or firmware.

69. Paragraph 6.8 claims that "the fraudulent firmware can to [sic] defend itself against parallel testing." That statement has no basis in fact. The claim in ¶6.9 that "cleverly designed firmware can detect differences in the patterns of use between testers and real voters" is pure fantasy. The patterns of use of voters and testers have never been captured, let alone evaluated. No one has ever published, or even purported to know, what the differences are, and Dr. Appel's claim that "these patterns can probably be effectively distinguished by standard methods of Computer Science," expresses merely wishful thinking, not even a reasoned expectation. In any event we ought to be quite safe in the intervening years before these discoveries are made, since they represent no present threat to any voting system. If Dr. Appel, turns out to be correct, however, his cautionary statement would also apply to DREs with VVPAT and optical scanners.

70. Dr. Appel writes in ¶6.11 that "it is actually quite straightforward computer programming to implement a program that works this way. It would take me or any trained programmer a month to write this program." Of course, Dr. Appel has not ever written such a program even though he had more than a month to perform his examination, and I now challenge him to do so such that the resulting program evades detection. It is my opinion that it cannot be done.

71. Parallel testing detects fraudulent firmware. It has been implemented in a number of states, including California, and is regarded as effective except by activists who are ideologically committed to eliminating DREs. Meanwhile, votes continue to be lost or altered in optical scan elections every year in the United States.

72. In summary, Section 6 reads like a science fiction novel. It sets forth a number of wildly improbable scenarios, then asserts without any demonstration whatsoever, or even an explanation, that it would be easy to create software to carry out those scenarios. The fact remains that no such manipulation is even known to have been attempted in a real election, and there is certainly no evidence that any attempt has succeeded. It is not even reasonable to suppose that attempts have been made, but have remained undetected. It is unlikely that the first attempt made by an intruder will succeed, or even succeed at evading detection. The reason is that malware contains bugs also, and when it is used in the field the first time, wildly unexpected behaviors may occur, much as the Sorcerer's Apprentice, thinking that he would simply animate a broom to assist him in sweeping the workshop, wound up generating an unbounded set of robotic brooms. Likewise, the first Internet worm, developed by Robert Tappan Morris, was detected because it went far afield and clogged the entire Internet – an unintended consequence. It is therefore to be expected that if people have really been trying to invade DRE machines, we would see a trail of failed attempts prior to a successful one. Yet there is no such evidence, which calls into question the very assumptions on which Dr. Appel's conclusions are based, namely that (1) it is highly desirable to manipulate elections; and (2) it is easy to spread undetectable software and firmware to do it.

73. While DRE cheating scenarios are complex and require a long chain of lucky events to succeed, no imagination or exaggeration is required to see how to steal votes in an optical scan election. Whoever gets his physical hands on the ballots can manipulate the election. This includes poll workers, employees who transport ballots to the county clerk, drivers, county workers and members of the resolution board who touch the ballots to look for write-ins and damaged ballots. In case of a recount, anyone who handles a ballot can alter it. When ballots are stored between the election and the recount, numerous people may be able to obtain access to them. Unlike Dr. Appel's malware scenarios, these are not theoretical but occur every year in the United States.

74. Section 7 claims that "the technical knowledge to write vote-stealing programs is basic computer science, widespread in our society. This is partially true, but misleading. Once a programmer is told what to write, it would be straightforward to program a vote-stealing program. However, it is not straightforward to design a vote-stealing program that is able to steal votes without detection, that maintains a demographic database with data about every upcoming elections (so it knows what percentage of votes may safely be stolen), to conceal itself from firmware verification procedures and parallel testing. No only has no one every done this, but no one has ever explained how it might be done. Thus the fact that programming ability is widespread says nothing about the ease with which impostor software might be introduced into a voting system without detection.

75. I observe that no technical skills whatsoever are required to steal or substitute bags of voted optical scan ballots, and this ability if much more widespread in our society than skill at computer programming.

76. Section 8 editorializes on the obvious danger of leaving voting machines unguarded where members of the public or intruders might obtain access to them. Of course this should not be permitted. The responsible solution is not, as Dr. Appel concludes, to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure. The responsible solution is to store the machines securely. I note that the physical insecurity Dr. Appel comments on is also applicable to DREs with VVPAT and optical scan systems, which also should not be stored where they might be tampered with.

77. Paragraph ¶8.6 claims that once installed, fraudulent firmware could cheat in every subsequent election. The obvious remediation is to ensure that the authorized firmware is reinstalled prior to each election at the time the machines are set up and sealed for that election. This remediation has been used successfully in Pennsylvania after the discovery of the Hursti optical scanning intrusion described earlier.

78. Section 9 describes the ease with which the lock on an AVC Advantage can be picked. The same is true of the lock on each voting machine of which I am aware, and every

optical scanner. This complaint misapprehends the purpose of such locks, which is not to defeat the determined intruder who is allowed to access the machine unobserved. It is to keep picky fingers away from sensitive areas of the machine when it is exposed to the public.

79. The notion that sequentially picking the locks on the 1200 Advantage machines in Bergen County, for example, as a mechanism for stealing an election is cartoonish in its impracticality. Even if each machine could be opened, its circuit boards exposed, a ROM substituted and everything closed up and resealed in just five minutes, it would take 6000 minutes, or 100 hours, to alter every machine. No credible scenario would permit an intruder to operate unobserved in a machine warehouse for 100 hours. Even if it occurred, parallel testing would immediately reveal the intrusion.

80. Section 10 discusses the insecurity of plastic strap seals. I agree that they are insecure. Tamper-evident tape would be much better. However, Dr. Appel misapprehends the purpose of these seals. They are not there to defeat the determined intruder who had unfettered secret access to the machines. Such a person could easily bring along a seal-making kit and replace every seal he had broken. The seals are there to deter opportunistic interference with the machine and to keep the public away from the machine's internals and to provide a record of when the machines were prepared for the election and by whom. They are not intended to be a substitute for careful oversight of the location in which the machines are stored. I note that Dr. Appel's comments on the insecurity of plastic seals are also applicable to DREs with VVPAT and optical scan systems.

81. Page 36 shows a signed reports tape from the February 5, 2008 on which the election officers failed to fill in the seal number with which the machine was sealed after the close of polls. It is odd that Dr. Appel would complain of this after have demonstrated how little security is provided by seals. The obvious remediation is to institute administrative procedures to force the officers to fill in the seal number. The responsible solution is not, as Dr. Appel concludes, to discard a system on which New Jersey has spent tens of millions of dollars and install one that is

less secure. I note that the same argument about results tapes can be made for DREs with VVPAT and optical scan systems.

82. Section 12 is similar to Section 5, except that it deals with the possibility of replacing the CPU chip of the Advantage instead of a firmware module. All of my comments regarding Sections 5 and 9 are applicable to Section 12. Not only would the intrusion be detected by parallel testing, it would take hundreds of hours to install. Furthermore, it could not conceal itself from a forensic examination either before or after an election, so evidence of the tampering would remain in the voting machines. If, as Dr. Appel opines, that fraudulent chips are a risk to election systems, they are also a risk in DREs with VVPA and optical scanners.

83. The speculation in Section 13 regarding possible motivations of potential intruders consists entirely of Dr. Appel's personal musings and is unsupported by any facts, data, experiment or demonstration made by him and therefore lacks any basis. The possibility that one might know in advance which particular precinct or county to tamper with in order to throw a presidential election is unreasonable. In the absence of such knowledge, any intrusion would have to involve multiple counties in multiple states and tens of thousands of voting machines. It would require numerous persons to conspire to commit numerous felonies and hope that no co-conspirator was either an undercover investigator or would turn state's evidence when arrested. This is no grounds on which to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure.

84. Section 14 leads the reader through a bogus path to an unjustified conclusion. Dr. Appel sets up an unreliable procedure for verifying ROM firmware. He then asserts, incorrectly and with no justification whatsoever, that there is no means to detect fraudulent firmware in the AVC Advantage.

85. I note that if Dr. Appel is correct that there is no way to verify firmware in the Advantage, then there is no way to verify firmware in a DRE with VVPAT, an optical scanner, or any other device on the planet that contains firmware.

86. It is true that it is not easy to very firmware in voting machines because the vendors have not made any provision in their system design to allow it. A port should be provided so that electrical tests can be performed on the processor chip and firmware chips without the need to open the machine and pry out the chips.

87. The notion that there could not be a trustworthy device to perform ROM verification is just silly. Such devices could be made by third-party providers and tested by and certified by independent laboratories and accounting firms. The firmware checker could be a custom chip whose contents are unalterable. The major parties could use devices made by different companies to run tests on the voting machines. If the parties' results agreed with each other, then all would be well. If there were a discrepancy, further investigation would be needed.

88. At several points in the Report, Dr. Appel quotes from the 2002 Voting System Standards (VSS) and the 2005 Voluntary Voting System Guidelines (VVSG), despite the fact that neither of these has ever been adopted in New Jersey. His quotations are selective: when he feels that a provision will help his cause, he cites it. Provisions that detract from his argument go unmentioned. The requirement of firmware verification is found in the 2002 VSS at 6.4.1(a): "If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations."[2] If such verification were impossible, as Dr. Appel claims, it would be useless to require it in the VSS.

89. Section 15 makes the obvious point that insiders have access to voting equipment. The fact that insiders have access to sensitive equipment (which is always true) does not in any way mean that such equipment is useless in elections. It is of course important to institute procedures to ensure that the insiders cannot mount the attacks proposed, or to ensure that any intrusion will be detected. In any event, parallel testing would reveal the intrusion, so there exist effective techniques to counteract the effect of such an attack. I note that the complaint made by

[2] Likewise in 2005 VVSG at 7.4.1(a).

Dr. Appel in Section 15 also applies to DREs with VVPAT and optical scanners. Insiders have access to those systems also.

90. Paragraph 15.2 asserts that Dr. Appel has "done extensive research and teaching on the history of election fraud in the United States." If that is true, then he knows that despite the fact that DRE machines have been used here since at least 1979, not a single case is known in which a single vote has been lost or stolen from such a machine my malicious intrusion. He should also know that every system that uses document ballots, including hand-counted paper ballots and optical scan ballots, have been victimized in every year by malicious intruders. Therefore, his conclusion that New Jersey should replace its current voting systems with optical scan does not comport with his own research into voting fraud.

91. Section 16 repeats the false premise that fraudulent firmware can be undetectable. It then goes on to offer a thoroughly misleading discussion of the actions of the Election Assistance Commission with respect to software independence and the voting system guidelines proposed by the TGDC.

92. "Software independence," which on its face sounds like a good idea, is nothing more than a codeword for "paper records.[3]" The reason for this is that the TGDC, which proposed the concept, says that it does not believe that any device can achieve software independence unless it maintains paper records (or records on some medium equivalent to paper, such as plastic.) Far from endorsing this concept, the EAC has withheld approving the proposed guidelines because it recognizes that they would require paper. The EAC has enough experience with elections to understand that completely auditable systems can be deployed that do not use paper records. It has thus been unwilling, and remains unwilling as of this date, to approve the guidelines.

93. The impasse is so severe, that the guidelines, which originally named the "2007 VVSG," and were supposed to be approved in 2007, now face little hope of approval. They have been renamed the "Next VVSG," because the EAC cannot predict in which year they might be in

[3] This is conceded Dr. Appel in ¶ 66.2 of his Report.

condition for approval, let alone implementation. Far from imposing a software independence requirement, it appears that the EAC will reject it.

94. Paragraphs ¶16.8-9 are an ad hominem appeal to authority. Dr. Appel cites a list of 52 supposed experts identified by an anonymous organization called the "Election Technology Library." Its website, www.electiontechnology.org, does not identify the individual who run the organization or what its policies, if any, may be. Of the list of 52, Dr. Appel himself selected 25 who he believes possess expertise in computer science or related technology. He then points out that 22 of his self-selected 25 "experts" have publicly expressed opposition to DREs that do not maintain paper records.

95. What can one make of this argument? It essentially says, "I have picked a list of people who agree with me, and they're smart people who know about computers, so regardless of the weaknesses in my arguments in this report, you should believe them." I suppose I should be honored to be one of Dr. Appel's 25 selected experts (and one of only two to have favored DREs without paper records), but I believe he chose me primarily to show that my opinions are not shared by his majority.

96. Brittain Williams and I are the two individuals out of 25 who Dr. Appel says disagree with his band of 22. If appeals to authority are to be the order of the day in the expert reports in this case, then I note that Dr. Williams has decades of experience in the administration of computer voting and for many years has had charge of the certification and distribution of voting system software and firmware for the state of Georgia, which has a uniform statewide voting system. Since 1980, I have performed more than 120 voting system certification examinations, more than any person in the United States. No one on Dr. Appel's list of 22 has experience comparable to mine or Dr. Williams'.

97. The statement in ¶16.10 concerning the policy committee of the Association for Computing Machinery is not "more evidence for consensus," as claimed by Dr. Appel. He fails to note that the policy committee was dominated by some of the 22 people identified in ¶16.9, so it is not "more evidence." It is the same evidence, and it is not evidence. The Association for

Computing Machinery does not focus on election administration, and its members in general know no more about elections than the average citizen.

98. The conclusion expressed in ¶17.1, namely that "No one approaching an Advantage voting machine in New Jersey – whether a voter, a party challenger, or an election official – can have any justifiable confidence that the machine is legitimately counting the votes" is not justified. Quite the opposite conclusion is warranted: there is no reason to believe (because there is no evidence of it) that any voting machine in New Jersey has not legitimately counted votes. Here Dr. Appel's scare tactic backfires, because his statement also applies to DREs with VVPAT and optical scanners. It also applies to hand-counted paper ballots, which are well-known to be susceptible to manipulation. Therefore, Dr. Appel's opinion implies that reliable voting in New Jersey cannot be conducted by any known method.

99. Part II of the Appel Report is devoted to a discussion of the security vulnerabilities in the WinEDS software and computers on which it runs. WinEDS is an election management system used to set up elections, create media for voting machines and to tabulate unofficial results on Election Day.

100. Dr. Appel makes sweeping statements about the potential of computer viruses throughout the Report, including in ¶17.2-17.6. It nowhere appears that Dr, Appel actually created such a virus, demonstrated that it could be inserted into an Advantage, or could spread from one Advantage to another. His discussion is therefore entirely hypothetical.

101. Paragraph 18.4 complains that the daughterboard of the AVC Advantage violates certain provisions of the 2002 VSS. New Jersey has not adopted the VSS and compliance with them is not a requirement for the certification or use of a voting system in New Jersey. But not requiring conformance to these standards by law, the New Jersey Legislature has impliedly determined that non-compliant systems can safely be used in New Jersey if they satisfy the other provisions of the Election Code. Possibly this issue should be revisited by lawmakers, but it is a matter to be decided by the Legislature. If the Court were to determine that compliance with the standards is necessary, then New Jersey should compel the vendor to supply a compliant system.

Non-compliance does not compel the conclusion that the state's voting system should be scrapped.

102. The vulnerability described in ¶¶19.1-12 is serious and of comparable magnitude to the Hursti optical scan exploit, which required immediate remediation when it was discovered in 2005. I agree that this vulnerability should be remediated forthwith. Ways of doing so are: (1) redesign the audio balloting method so that no software can be rewritten from the audio cartridge; (2) disable audio voting (and correcting the vulnerability described in Section 26); or (3) ensure that all audio cartridges are securely distributed and installed from a central location managed by state election officials.

103. I do not agree that the "second method" of tampering described in ¶¶19.14-15 is particularly serious because it only affects votes cast via audio and it requires individual, deliberate and malicious intrusion into each machine to be affected.

104. Sections 20, 23, 27 and 28 (and later, 40) are based on a common misconception, namely that the tabulation function performed by WinEDS on Election Night can affect the outcome of an election. In New Jersey it cannot. Winners of elections are determined by the canvass described at §19:19-8ff. of the Election Code. They are not determined from any unofficial results or reports produced by WinEDS. The canvass proceeds from the signed precinct totals produced at each polling place. Therefore, if someone tampers with the election results on the WinEDS computer, this will have no effect on the outcome of any race.

105. Nevertheless, I agree that voting machines and computers on which election management software is installed should never in their lives be connected to the Internet. It is easy to implement this policy by disabling and/or removing the computers' network interfaces and software for communicating over the Internet. It is not necessary to scrap New Jersey's entire collection of voting machines and election computers.

106. The discussion in Section 21, 22, 25 and 28 are notable in that Dr. Appel never states that he ever created any virus or demonstrated that the program he did write could spread from one machine to another.

107. The conclusion in ¶23.15, that "WinEDS is highly vulnerable to tampering, and there is no simple way to make it invulnerable," is not correct. The methodology described above to make it impossible to connect the WinEDS computer to the Internet, will suffice to protect it from Internet intrusions and Internet-borne viruses.

108. With respect to ¶23.17, changing ballot definitions on the WinEDS computer may cause inconvenience, but will not ultimately affect the election. Ballot definitions are (or should be) checked carefully by the parties when the machines are prepared for an election. Parties are vitally interested to ensure that all of their candidates are on the ballot and in the proper positions.

109. The vulnerability described in Section 24 can be remediated by the method discussed above concerning audio cartridges.

110. Section III of the Appel Report ostensibly deals with the Advantage user interface.

111. In ¶28.3, Dr. Appel maintains that using the Advantage can "allow pollworkers to collude with voters to perpetuate vote fraud." He fails to note that collusion between voters and pollworkers can lead to vote fraud regardless of the type of voting system this is being used. It is much easier, in fact, to engage in vote fraud using the optical scan system Dr. Appel proposes than with any DRE.

112. Section 30 comments on potential loss of votes by having voters vote on the Advantage when it is not activated for voting. The machine responds by briefly lighting up lights next to candidates selected, and when the "Cast Vote" button is pressed, appears to record a vote. But it does not. The behavior is probably best described as a "misfeature." The reason the machine responds to button presses when not activated is so that election officials can verify that the machine is working without having to activate it for voting, which would cause an unauthorized vote to be cast and play havoc with the audit trail that is counting the number of activations. There is good reason for the machine to be able to be tested between voters.

However, the behavior programmed into the Advantage for this testing is confusing and risky. It was the subject of a portion of my Pennsylvania examiner's report in May 2006.

113. There is a discernible difference in the behavior of the machine when it is activated for voting and when it is not. When not activated, the candidate light stays on for a fraction of a second only, then goes out. This is for testing purposes. When the machine is activated, the candidate light stays on. From my experience in elections, I judge that the probability that a voter would (1) be confronted with an unactivated machine; and (2) fail to notice that the voting booth lamp is out; and (3) press candidate selections and fail to notice that no lights were lighted; and (4) quickly press the "Cast Vote" button and leave the booth; and (5) have the pollworker not realize that the machine was not activated during voting to be essentially zero.

114. The inter-voter behavior of Advantage should be changed. However, the possibility of occasional confusion is no justification for scrapping the state's voting system and spending $100 million[4] on another one whose user interface is even worse. Dr. Appel omits to mention that the voter is provided with no feedback whatsoever while she is filling out an optical scan ballot, is not warned of overvoting or undervoting, does not receive instructions or guidance through the ballot, and is not compelled to review her choices before casting a vote. Dr. Appel has conducted no examination or study of possible voter confusion in the user interfaces of the systems he proposes as alternatives, namely DRE with VVPAT (which has a much more confusion interface than DRE without VVPAT) and optical scanning, which effectively has no user interface at all.

115. There are two simple remediations for the confusing behavior of the Advantage: (1) the pollworker should not allow the voter to touch the machine until it has been activated for voting; and (2) the voter should be instructed to ensure that the public counter advances by one after they have voted. If any question arises whether the vote has counted, it can be resolved by

[4] I have been informed that it would cost approximately $100 million to deploy precinct count optical scanning throughout New Jersey.

comparing the public counter to the number of Activation Tickets collected for that machine. I think these measures can be implemented for far less than $100 million.

116. The behavior described in Section 31 is indeed bad, relating to the ability of a pollworker deactivating the machine after it has been activated but before the voter votes. Rather than spend $100 million for a new voting system, I suggest that New Jersey remediate the situation by offering the following instruction to voters: "While you are voting, make sure the light in the voting booth remains on at all times. If the light is off, your vote will not be counted. If the light goes off, notify an election official immediately."

117. It is recognized by statute that all voting systems have deficiencies of various kinds, and that these can often be alleviated through administrative rather than technical means. The Help America Vote Act, to which New Jersey is subject in elections for federal office, provides that in some circumstances the failure of a system to comply with the statute may be remedied by a state by "establishing a voter education program specific to that voting system" or "providing the voter with instructions." 42 U.S.C. §15481(a)(1)(B).

118. Section 32 is an over-the-top complaint about the failure of the Advantage to use different audible sounds so that bystanders can tell the difference between an activation of the voting machine and the casting of a vote. Dr. Appel worries that a corrupt pollworker could activate a machine twice for a particular voter and others in the vicinity might not realize what is going on. But this is not true. Anyone who observes a voter at the machine will hear four sounds (two activations and two "cast vote" indications) if the voter is allowed to vote twice. The observer will only hear two sounds for a single vote. The difference between four and two is quite apparent. And Dr. Appel presents this right after having explained in Section 29 the elaborate procedure used in New Jersey to thread the voter's Voting Authority ticket onto a string attached to the machine. If voters vote more than once, the number of votes cast will not correspond to the number of tickets, and the irregularity will be discovered.

119. Neither the New Jersey Election Code, HAVA, the 2002 VSS or the 2005 VVSG requires any audible indication of the activation of the machine or the casting of a vote.

120. Dr. Appel fails to note that voting multiple times in a precinct count optical scan system is much easier. The pollworker need only allow the voter to feed multiple ballots into the machine.

121. Section 33 discuses undervote rates in certain offices . I do not understand Dr. Appel to be offering an opinion that full-face DREs are non-statutory, unconstitutional or that they violate any know set of standards or guidelines for voting machines. I note further that Dr. Appel has performed no comparison, and has not cited any study performed by other, measuring the undervote rates on DREs with VVPAT or precinct count optical scan systems that he proposes as alternatives.

122. Paragraph 33.3 cites a brief paper by Prof. David Kimball containing statistics about undervote rates on various machine used in New Jersey. A reader of the Kimball paper will find that, unlike Dr. Appel, Dr. Kimball did not speculate or jump to conclusions about the cause of the undervote.

123. It is true that the user interface on the AVC Advantage is not effective in warning the voter that she has undervoted. The question is what can be done about it, not to ask New Jersey to spend $100 million to reduce undervoting, especially when there is no proof offered that such an expenditure would even have the desired effect. To me, the answer is simple – the vendor should be compelled to produce a better interface, or risk the loss of New Jersey's business. Until such an improvement or retrofit can be accomplished, administrative remediation is feasible.

124. In ¶33.5, Dr. Appel says that the lack of a video screen for communication to the voter may be a possible cause for the observed high undervote on public initiatives. If he is correct, the situation can be no better for the optical scan systems he proposes as replacements, since they do not communicate with the vote by any means whatsoever while the voter is marking her ballot.

125. Standards applicable outside New Jersey (e.g., the 2002 VSS) require that a DRE voting system "indicate to the voter when no selection, or an insufficient number of selections,

has been made in a contest." 2002 VSS §2.4.3.3(e). The Advantage satisfies this requirement by keeping the office block illuminated for an office until that office is no longer undervoted. It is of course possible to provide a more prominent or better indication, but it cannot be said that the current method unconstitutionally disenfranchises voters.

126. Section 34, entitled "Voter can't tell which primary is activated" contains false and misleading statements. Dr. Appel states that "Inside the booth, there is no indication, on the full-face preprinted ballot, or which party's primary is activated." However, there is indeed such an indication, as shown and explained by Dr. Appel at approximately 10 minutes into his DVD presentation, where he explains that only one of the two primary ballots on the face of the machine is activated, and the voter can determine which one it is by attempting to select a candidate. No candidate can be selected on the ballot that is not active. Dr. Appel also fails to note that the voter's LCD display at the bottom of the ballot shows which ballot has been activated. The correct title of Section 34 should have been, "Vote CAN tell which primary is activated."

127. Section 35 moves into the realm of the ludicrous as Dr. Appel becomes more desperate in his quest for optical scanning. He complains that a pollworker who peeks through certain slits in the Advantage while a voter is voting can learn the voter's choices. Of course the same thing is true of lever machines if the pollworker peeks through the privacy curtain. It is also true of optical scan voting if the pollworker stands behind the voter and watches. No voter will allow this. If a poll worker is thought to be observing a voter, the voter may immediately raise the hue and cry that the pollworker is committing a crime of the third degree (§19:34-13, (§19:53A-15), a felony.

128. Of course, Dr. Appel proposes that the response to this risk is to buy a new voting system for $100 million instead of simply instructing voters that pollworkers are not to stand near the voting machine while the voter is voting.

129. I note that Dr. Appel has not performed any experiments, nor has he cited any references, dealing with the comparative privacy of the AVC Advantage and the systems he proposes as replacements.

130. I agree with the observations in Section 36 concerning the inability of a voter to cancel a "personal choice" (write-in) selection after pressing "ENTER." I have commented adversely on this behavior in several of my official examiner's reports in Pennsylvania. The inability to review and correct write-ins easily is a significant flaw in the Advantage interface. However, it is not illegal. HAVA requires that a voting system shall "provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error)." 42 U.S.C. §15481(a)(1)(A)(ii). The voter who finds the need to review or correct a write-in can ask the pollworker to deactivate the machine and active it again, which is analogous to the procedure for obtaining a replacement optical scan ballot. This process is inconvenient, but statutory.

131. Section 37 complains that it is possible, if pollworkers do not follow proper procedures, to learn the choices left by a fleeing voter. Of course, to do this they must not only ignore directives, but also commit a felony in the process.

132. Dr. Appel says that "this issue slightly impairs the accuracy of the AVC Advantage in recording the voter's intent." This is incorrect. The intent of a fleeing voter cannot be determined. It is possible that the voter left the both intending not to cast a vote at all (yet did not understand how to de-enable her selections), or she may simply have left intending to vote but inadvertently failing to press the "Cast Vote" button.

133. Polling place procedures determine whether the ballot of a fleeing voter will be counted, by having a pollworker reach around (without looking) and hit the "Cast Vote" button, or whether the ballot will be voided by deactivation. In either cease there is no necessary violation of privacy.

134. There is no practical difference between this situation and that of a voter who leaves an optical scan ballot on the floor of the polling place instead of handing it to a board member. Anyone who sees the voter and the ballot has some information about the voter's choices.

135. The answer is simple: TELL VOTERS NOT TO FLEE. Then the problem goes away.

136. Dr. Appel's conclusions in ¶38.3 are not justified by anything in his Report. Disenfranchisement, if it occurs, is a serious problem. However, it does not implicate either accuracy or security, as claimed by Dr. Appel. "Accuracy" refers to the ability of a voting system to tabulate correctly every valid vote cast. If, for some reason, a voter is not able to cast a valid vote, that is not an accuracy issue. I cannot determine in what way the issues discussed in Sections 28-38 have anything to do with security.

137. Section III deals with design errors and software bugs.

138. Paragraph 38.4 repeats the incorrect assertion that the attacks described are undetectable by audits. That is not true if the audits include parallel testing.

139. Much of Section II contains Dr. Appel's conclusion as to the "inadequacy" of various features of the Advantage. His definition of "adequate" appears to be synonymous with "perfect." One would not regard the lock on a bank vault as insecure if high explosives could be used to blow the door open. One might regard the lock as insecure if its combination could be readily discovered, the door had no time lock, was not guarded and was not subject to video surveillance. Somewhere between the two extremes the security level makes the transition from adequate to inadequate.

140. The same applies to voting systems. Perfection is never the appropriate standard, and to insist on it is to mandate failure. Even if computer security were the only issue to be considered in evaluating voting systems, and it is not, it would still be impossible to build completely trustworthy systems , or build them at any reasonable price.

141. The fact that judgments must be made about the safety of a voting system is recognized by statute. The New Jersey Election Code relegates the determination to the Secretary of State. None of the statutory requirements in §§19-48 and 19-53 is phrased in absolute terms. For example, §19-48-1(a) states that the machine "shall secure to the voter secrecy in the act of voting." That does not mean that every voter's vote must remain absolutely secret under all conceivable circumstances, or that the county must provide armed guards to shoot people who try to peek into a voting booth, or that ballots must made of material to which fingerprints and DNA will not adhere to prevent genetic testing from being used to compromise privacy. It does not mean that election officials must sweep the polling place to detect hidden video cameras and surveillance devices that might be used to discover how people are voting. While each of these intrusions is conceivable, no one except Plaintiffs believes that every conceivable risk, including risks that have never occurred, must absolutely be prevented by a voting system.

142. In ¶39.2, Dr. Appel asserts that the mechanisms used by Sequoia are "completely inadequate" for the purpose of validating the integrity of vote data. While they do not perform the function that Dr. Appel wishes they might perform (which is not required by statute), the do provide protection against certain events that would cause vote date to be changed.

143. While no one wants people successfully altering the contest of results cartridges, even if this were to happen it would not be fatal to the election. Vote data on the results cartridge is also stored on the Advantage itself in non-volatile memory having a lifetime exceeding 20 years. (Dr. Appel does not mention this in his Report until p 121.) If someone were to modify the data on the results cartridge, it would be revealed in an audit because a new results cartridge could be written from each Advantage machine, and the data on the new cartridge compared with the one removed on Election Night. Therefore, the apparently horrific risks detailed in Section 39 and 40 are in fact non-existent. In particular, the reading of results cartridges by WinEDS produces unofficial totals only and does not affect the outcome of any race.

144. Section 41 does not reflect how the canvassing process works in New Jersey. The "use" of electronic totals by county clerks is for unofficial purposes only, and is not used to determine official winners. That is done using the very paper results that Dr. Appel says should be used. In any event, even if it is not, it would be a simple administrative change to have county clerks act otherwise. The statement in ¶41.7 that "errors and fraud in Results Cartridges will influence official election results" is factually incorrect.

145. The manipulation described in Section 42 is unrealistic and in any case would be detected and also can be prevented by administrative measures. The hypothesis is that an unscrupulous pollworker possesses a fraudulent results cartridge, places it into the Auxiliary port of the Advantage, and causes the vote totals from the Auxiliary port to be printed instead of those from the real results cartridge. I assume for the moment that all of these acts could be carried out without being noticed at the time they occurred. The pollworker and his accomplices have no way of knowing how many voters have voted on that machine in time to make a suitable substitute cartridge. Furthermore, unless he removes the sealed original results cartridge from the machine, he cannot produce a phony cartridge that will be accepted at the county tabulation center. The results tape will show a number of votes that does not correspond to the sign-in records maintained at the polling place. If he sends the real results cartridge to the county, the fraud will be detected, so he must steal the original cartridge. However, the contents of the real results cartridge remain in the machine. If the results are audited against the non-volatile records in the machine, the fraud will likewise be discovered.

146. Administratively, it is wise of course not to permit anyone to get his hands on a voting machine on Election Day outside the presence of witnesses.

147. The manipulation described in Section 43 cannot be carried out in practice, would be easy to detect, and there is no indication that Dr. Appel even attempted to carry it out during his examination of the Advantage. The first thing that is wrong is that any effort to conceal the results of the fraud by manipulating the printout at the precinct will immediately be detected

when the results are tabulated at the county tabulating center. The reason is that the report lines that Dr. Appel seeks to suppress cannot be suppressed in WinEDS.

148. Detection of this fraud is easy. All one need do is, at any time during Election Day when the machine is turned on, depress each button on the machine and observe the contents of the LCD display, which will give the name and party of the candidate. If any button causes a candidate name to be displayed but no candidate name appears on the printed ballot face opposite that button, then something is wrong. This check is normally performed during pre-LAT to ensure that the ballot setup is correct.

149. Another method of detecting the fraud is simply to compare the total number of votes cast for all candidates in an office with the total number of voters who voted. Any more than a trivial number of double votes will be caught.

150. Another method of detecting the fraud is to examine the results cartridge at the tabulating center to verify the ballot setup. It will immediately be apparent (since a candidate's name will appear in more than once place), that the ballot setup does not conform to that of the official election.

151. I do not agree that the exploit in Section 43 represents any sort of real risk. Nevertheless, I agree with the statement in ¶43.6 that the ballot definition should be checked for well-formedness by the software before it is used.

152. The manipulations described in Section 44 represent no real risk. Dr. Appel here tries to make much of the fact that one type of Results Cartridge can be transformed by an unscrupulous person into any other type of Results Cartridge, even a Technician Cartridge. But this is no indictment, since numerous such cartridges exist and it would be easy to appropriate a legitimate one without having to cut wires on circuit boards.

153. The manipulation described in Section 45, namely the possibility that a pollworker might alter the totals contained on an Early Voting Cartridge, even though early voting is not legal in New Jersey, is not well-founded. It is always true that if an insider can gain access to election records and alter them, the election can be corrupted. This is true as well of

optical scan ballots. If a pollworker can later the ballots then there is no way to reconstruct the election. The remedy is to institute procedures so that insiders cannot gain unobserved access to crucial documents, files or records.

154. The manipulation described in Section 46 is of no particular consequence because (1) no winner is declared based on the contents of Consolidation Cartridges; and (2) the original correct election records remain on non-volatile memory inside the Advantage and are available for audit. The conclusion in ¶46.5 that "Consolidation Cartridges allow many opportunities for stealing votes," evidently intended to scare the Court, is factually incorrect. Not a single vote can be "stolen" using a Consolidation Cartridge.

155. I note that Dr. Appel does not claim to have performed the manipulation described in Section 46. Therefore, he has not shown that it would be feasible, and in particular has not shown that it would be feasible in a real election setting.

156. Nevertheless, I agree that Advantage and WinEDS should check cartridges for the presence of negative vote totals. I do not agree that the present vulnerability of Consolidation Cartridges justifies scrapping an entire voting system.

157. The manipulation described in Section 47 is easily repelled. Of course if it were possible to manipulate voting systems wirelessly that would represent a huge risk. It is therefore important to ensure that wireless components are not introduced into voting machines. The attack of Section 47 can be prevented by imposing administrative controls to keep unauthorized cartridges from being inserted into voting machines. All voting systems require some degree of physical security against intrusion. It is always true that if one can replace the components of a voting system with rogue devices, then the election can be compromised. This is also true of DREs with VVPAT and optical scanners.

158. I note that Dr. Appel does not claim to have performed the manipulation described in Section 47. Therefore, he has not shown that it would be feasible, and in particular has not shown that it would be feasible in a real election setting.

159. The manipulation described in Section 48 I the same character. If someone can replace the machine's components, the machine no longer operates as intended. It is elusive what the significance of this observation might be. If someone replaces the voting machine with an imposter machine, the election can be compromised. The solution is not to ban voting machines, but to ensure that such substitutions do not occur.

160. Possibly the point of Dr. Appel's discussion in Sections 39-48 is to suggest that the substitution of components is so easy that the systems are so fatally insecure that they should never be used.

161. The privacy attack discussed in Section 49 demonstrates the huge deficiencies in Dr. Appel's investigation. He never troubled to compare the Advantage with any other system whatsoever, including the systems he proposes as replacements. The privacy of voters is completely compromised by DREs with sequential paper-tape VVPAT. Dr. Appel concedes this

162. The privacy of voters is also compromised by precinct-count ballot scanners, and without the use of surreptitious sound recording devices or any other technology. Before the first voter puts her ballot through the scanner, the ballot box is empty. Without doubt, her ballot ends up on the bottom of the box. The next ballot winds up on top of the first. While the ballots do not fall neatly into a sequential pile (because the cross-section of the ballot box is larger than the outline of a ballot and there is some randomness to the ordering), the last ballot finishes on the top of the box. Therefore, when the ballot box is opened it is easy to see how at least the first and last voters voted, in violation of statute.

163. The exploit of Section 49, which requires significant labor, technological sophistication and commission of felonies, is vastly less likely to be successful than either of the privacy attacks against VVPATs or optical scanners. So silly is the proposed attack, when viewed in comparison to the rampant privacy compromise of Dr. Appel's suggested replacements, that I will not even bother to take issue with its practicality. I observe that a much easier attack is to mount a high-resolution video camera in the ceiling of the polling location to watch everything each voter does in the voting booth. Does the possibility of such surveillance

imply that we should no longer vote in polling places, or that we should no longer vote at all? Yet this is essentially what Dr. Appel is saying: "I have invented a privacy exploit that works against the Advantage, so the Court should force the state to adopt a system in which much easier exploits are possible."

164. I note that Dr. Appel does not claim to have performed the manipulation described in Section 49. Therefore, he has not shown that it would be feasible, and in particular has not shown that it would be feasible in a real election setting.

165. The conclusion of Section IV, expressed in ¶50.1, that cartridges "can be manipulated to steal votes," does not follow from the examples given by Dr. Appel. While unofficial totals might be interfered with, no stealing of votes (removing them from the system so they cannot be reconstructed) has been demonstrated.

166. Part V is devoted to criticism of Sequoia's software design practices. At the outset, I agree that those practices are poor and in need of improvement. However, bad design methodology does not necessarily result in erroneous software. Even Dr. Appel does not claim that the practices resulted in error. Instead, he observes that they "increase the chance that these mistakes will slip through review and certification processes. Mistakes in the program can either directly miscount votes or can open security vulnerabilities that allow attackers to steal votes."

167. In all of Part V, Dr. Appel never actually identifies any such mistake or claims that any exist. And, as already explained above, mistakes of the type discussed by Dr. Appel do not "steal" votes, however appealing that analogy may seem.

168. The code of the Advantage indeed does not follow best software engineering practices, as claimed by Dr. Appel in ¶51.1. However, that by itself does not mean that the software contains errors.

169. Paragraphs 51.5 and 51.6 complain that the Advantage source code violates various software design principles mandated by the 2002 FEC Standards. First, the FEC Standards do not apply in New Jersey. Second, the issue whether a system that has been granted

a qualification letter by an Independent Testing Authority as having conformed to FEC Standards actually conforms to those standards is not before the Court.

170. I agree that not conforming to standards makes it more likely that a program will contain errors, and may make those errors harder to discover. However, I note that Advantage has been examined by an Independent Testing Authority, has been certified in New Jersey and having been used successfully over a period of years in multiple jurisdictions, including New Jersey. There is no allegation that it contains any coding errors that would alter any vote totals, so there is no basis on which to conclude that it should be replaced by a different system.

171. Section 52 comments on the inadequacy of the Wyle Laboratories' ITA examinations. I do not quarrel with the observation that ITA procedures are frequently ineffective. In fact, I have so testified before the U.S. Congress. However the issue is what is the correct forum in which such examinations should be reviewed. The Voting System Testing Laboratories (VSTLs), formerly known as ITAs, are reviewed by NIST and certified by the EAC pursuant to HAVA. The appropriate remedy, if the actions of a VSTL are considered inadequate, is to seek at the EAC level to have the VSTL decertified. It is unreasonable to expect the courts of the individual states to review the certifying procedures of the EAC and to make possibly inconsistent determinations regarding the validity of action by the VSTLs.

172. Section 53 speculates that New Jersey did not consider ITA reports. It is unclear what the factual basis for this speculation might be, since I am not aware than anyone involved in certifying voting systems has either been deposed or has provided any statement detailing what materials might or might not have been considered. Dr. Appel fails to note that New Jersey does not require ITA qualification, so it has no obligation to seek, read or consider any ITA reports.

173. I am at a loss to determine how the opinions in Section 54 relate in any way to the question whether the AVC Advantage may constitutionally be used in New Jersey. If Plaintiffs believe that Sequoia has not fully complied with a discovery request, it seems that a motion to compel might be brought. The conclusion in ¶54.13 that "Sequoia has no effective way of knowing whether they have installed tainted software in the AVC Advantage" is not justified.

There is no evidence, nor do Plaintiffs even suggest that any such evidence may exist, that would indicate that tainted software has ever been installed in an AVC Advantage anywhere on Earth (except during Dr. Appel's experiments). On the contrary, the software has been tested and used successfully on numerous occasions without any hint of taint.

174. The "conclusion" of Section 55 is that "Sequoia's sloppy software practices can lead to error and insecurity." In the entire 169 pages of his report, however, Dr. Appel fails to identify a single error or insecurity that might have resulted from Sequoia's software practices.

175. Part VI is devoted to a discussion of the circumstances leading to voters' being presented with the wrong primary ballot in the election of February 5, 2008. I do not dispute Dr. Appel's explanation of the cause of the 37 miscast votes. There is a bug in the Advantage software which, when exercised by having the pollworker press an incorrect button, causes the wrong primary ballot to be activated on the machine. There is no way to claim that such a bug is acceptable. However, it can easily be remediated by a physical modification to the operator's panel to make the incorrect button impossible to press. Thus the effect of the bug can be eliminated completely.

176. I note further that there is no difference between the poll worker activating the wrong ballot on a voting machine and handing the voter the wrong optical scan ballot. Both can be done inadvertently or deliberately. The voter ought to notice that none of the candidates she intended to vote for appear on the ballot. Adopting the optical scan replacement advocated by Dr. Appel would not alleviate the problem. If the Advantage is remediated as described above, there is no greater chance of a pollworker energizing an incorrect ballot on it than handing the voter the wrong paper ballot.

177. Section 57 is concerned with the obvious point that if a voting machine fails just as a vote is being cast, it might not be easy to determine whether the vote was recorded or not. That does not mean it is impossible, as claimed. After the polls are closed, the results in the machine's internal memory and the results cartridge will either agree or disagree. If they disagree, the memory containing one more vote than the other will have recorded the vote. If

they agree, then the totals number of voters who voted can be compared with the string of activation tickets to determine whether any vote is missing. How does this help the voter, who went home a long time ago? One possible answer is to use provisional balloting. If it cannot be ascertained while the voter is present whether the ballot was counted, the voter can cast a ballot using the provisional ballot mechanism[5]. If the original vote turns out to have been counted, the newly cast ballot would be discarded. If the original was not counted, the new one can be tabulated. While this mechanism is quite cumbersome, the circumstance under which it might be invoked is so rare as to have negligible probability.

178. The statement in ¶57.21 that "it is impossible to know whether the vote has been recorded" when the machine fails as the vote is being cast is factually wrong. As explained above, it can readily be determined after the close of polls. By using the provisional balloting mechanism, there is no risk of disenfranchising voters, or permitting them to vote twice, as claimed by Dr. Appel.

179. I note that there is no evidence that the failure described by Dr. Appel has ever occurred in an election in the United States. While it is hypothetically possible. the chance of it happening is so low that to require every voting machine to be completely resistant to it is to impose a standard of perfection far in excess of the "safety" standard of the New Jersey Election Code. Even the 2002 VSS and the 2005 VVSG permit a certain small percentage of ballots to be counted in error, because the authors of these documents recognize that neither humans nor mechanical devices can behave perfectly. Yet this is what Dr. Appel would require.

180. The conclusion in ¶57.22 that optical scan ballots provide some advantage in this regard is incorrect. The presumption that it is apparent whether a ballot has been deposited in the scanner does not in any way ensure that the ballot has been counted. After all, the results cartridge in the optical scanner is no more reliable than the one in an Advantage. The argument that all the ballots are safely stored in the machine and can be removed and recounted later has proven to be incorrect in every election cycle in which optical scanners have been used. There is

[5] This would not be a "provisional ballot" as that term is defined in the New Jersey Election Code. It would simply be cast using the provisional ballot mechanism provided by the system.

virtually no physical security surrounding ballot handing in polling places, and there is also scant protection against the feeding of multiple ballots into the scanner.

181. The "disenfranchisement" described in ¶58 is no worse than any disenfranchisement by handing the voter the wrong ballot.

182. Section 60 argues that different Advantage versions have different properties and therefore each version should be subject to separate examinations for approval in New Jersey. I agree with this general proposition. Paragraph 60.3 quotes language from NJSA §19:53a-4, namely that reexamination of a voting system is not required by reason of an "improvement or change which does not impair its accuracy, efficiency, or ability to meet such requirements." The Pennsylvania Election Code has a similar provision, which I have been involved in interpreting since 1980 in my capacity as statutory examiner: "When an electronic voting system has been so approved, no improvement or change that does not impair its accuracy, efficiency or capacity or its compliance with the requirements hereinafter set forth, shall render necessary the reexamination or reapproval of such system." 25 P.S. §3031.5(d). In practice the way this provision is implemented is for the vendor to disclose what changes have been made. A letter is usually solicited from an ITA stating that the changes have been examined and found not to affect the accuracy, efficiency or capacity. In any case, the Secretary of the Commonwealth makes a determination whether a new examination is needed. Clearly there are changes which do not require reexamination, such as replacing a power supply with a newer mode, changing the color and wattage of bulbs in the systems, etc. Software changes are always suspect because complex interactions can occur between portions of code that seem to have nothing to do with vote counting and other sections of the code. If Dr, Appel's point is that New Jersey should comply with its own statutes, I am in agreement.

183. Section 61 appears to be asserting a new cause of action in an expert report, which is procedurally unusual. I did not understand from the pleadings in this case that Advantage Version 10, which is not currently in use in New jersey, to be the subject of any claim for relief.

To the extent that Dr. Appel argues that New Jersey ought to comply with its own statutes, I am in agreement.

184. Section 62 deals with inferences made by Dr. Appel concerning the Advantage Version 8 firmware, which he did not examine. I assume, solely for purposes of argument, that his inferences are correct. Even so, his conclusion is unjustified.

185. In Section 63, to the extent that Dr. Appel argues that New Jersey should comply with its own statutes, I am in agreement. I do not agree that the 50 states and the District of Columbia should be conducting their own separate security examinations. This is wasteful and, on the few occasions on which different states have acted independently, contradictory results were obtained. (State A found a system to be secure, while State B decertified it.) I agree that all voting systems should be examined by skilled computer-security experts, but this examination should be part of the Federal certification process and not left up to the states.

186. The conclusion of Section 64, that New Jersey should not continue to use the AVC Advantage 9.00 because it is insecure, is unjustified and irresponsible. I have stated many times in the report that the mature solution to observed insecurities is to plug them, not to discard one system in favor of one that is less secure, like optical scan.

187. The conclusion of Section 65, that the audio kits should be removed, is not only unjustified, but offensive. It is typical of anti-DRE activists to care nothing for the effect their recommendations may have on the disabled (e.g. insisting on VVPAT systems that are invisible to the visually impaired). Removal of the audio kits in any event would violate HAVA. 42 U.S.C. §15481(a)(3)(A) requires that a voting system used in elections for federal office shall " be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters." Computer security experts like Dr. Appel tend to focus solely on the security aspects of voting systems and ignore everything else, including mandatory statutory requirements.

188. Section 66 again discusses the concept of "software independence," but it is not described correctly. NIST has defined software independence to mean "that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results." Some people, including Dr. Appel, claim that this implies that paper records are the only mechanism that provides software independence, but this is not the case. The Prime III system, developed at Auburn University, achieves software independence without a VVPAT.

189. The statement in 66.4 that "someone who wishes to cheat will have to ensure that a fraudulent firmware miscount come out exactly the same as the fraudulent paper recount" is incorrect and does not comport with New Jersey law, which provides that in the even of any discrepancy between electronic records and paper one, the paper records govern. This means that the electronic count will be discarded, so it does not matter whether it is the same as or different form the paper count. This is a weakness in VVPAT statutes. It may well be that the paper records have obviously been tampered with, but they must nevertheless be counted.

190. Paragraph 67.2 observes that it is the overwhelming consensus of "those computer scientists who have studied voting technology" that precinct-count optical scan is the most reliable form of voter-verified paper ballot. A more accurate statement would be that the 22 computer scientists hand-selected by Dr. Appel agree with him. I am not aware of any survey that has ever been taken of computer scientists on this point, and I dispute that it would be competent evidence. In fact, from 2003-2006 this same group of computer scientists insisted that the most reliable form of voting was the Mercuri method, namely DRE with a paper trail. When the severe drawbacks of that method became apparent (e.g. total loss of voter privacy), the computer scientists changed their mind. Possibly when they learn of the security vulnerabilities of optical scan voting, which they have never studied, they may change their minds again.

191. Far more competent are the opinions of election officials who have devoted their careers to administering elections. They, far more than computer scientists, are familiar with the real risks of voting that can be manifested in a real election setting rather than a laboratory.

These professionals are not clamoring for a change in voting method, though virtually all of them would favor administrative changes to make voting more secure.

192. The supposed advantages claimed by Dr. Appel in ¶¶67.5-11 for optical scan systems are not advantages at all. First, in optical scan there is no machine or computer program to assist the voter in moving through the ballot. There is no device to alter the voter to undervoting or overvoting[6], or to tell the voter whether the mark she makes will be recognized as a vote.

193. Each state was required under HAVA to define "what constitutes a vote." For optical scan systems this means a set of rules defining which marks on a ballot are to be counted as votes. These rules differ from state to state and both pollworkers and voters are usually completely unaware that they even exist. This means that voters can easily make marks on their ballot that they believe will count as votes, but which will not be recognized by the scanner and will not even be tallied in a manual recount. There is no effective way to warn the voter that she has done this. "Disenfranchisement by variant marks is a real problem that occurs far more frequently that any form of DRE disenfranchisement cited in Dr. Appel's Report.

194. The statement in ¶67.10 that "there can be no doubt about the selections written on an optical scan ballot" is false. Sometimes teams of well-meaning humans are unable to determine what an optical scan voter intended by her marks. This situation occurs frequently, and even occasionally affects the outcome of an election. Control of the entire Pennsylvania House of Representatives came down to a disputed race in a single optical scan county in 2006. The difference in vote totals between the candidates was approximately 20. A recount was conducted and about 50 ballots were found having questionable marks. A court attempted to interpret the ballots and was able to do so in enough cases to declare a winner. However, to this day approximately 12 ballots remain on which is it still unclear which candidate the voter intended to select. So it is not true that optical scan ballots remove doubt about voting choices.

[6] Optical scanners can be set to reject an overvoted ballot. In my experience, the result is that the voter is usually too embarrassed to request a new ballot, and asks that her ballot be counted anyway. Optical scanners are almost never set to reject undervoted ballots because this would result is large percentage of rejections.

195. The fundamental error made by my computer science colleagues in favoring optical scan systems is that no such system provides for any backup whatsoever. There is one and only one original ballot. There are no copies[7]. If anyone alters, removes, or augments the ballots there is no conceivable way to reconstruct the election or perform a recount. This is not a hypothetical argument. In each election cycle, voted ballots are found in some jurisdiction weeks after the election whose chain of custody cannot be established. It is the easiest possible manipulation to fiddle with pieces of paper because no training or education is required.

196. In DRE systems, multiples copies of the ballot images ("cast-vote records") are maintained in separate memories. Some of these memories remain in the voting machine that received the votes. Others are removable and can be tallied elsewhere. Once the removable memory is no longer in the machine, and assuming that the vote recording mechanism is working properly (which can be verified), a would-be intruder cannot change all of the memories so that they are identical with one another. This inherent redundancy affords very powerful protection against fraud.

197. An optical scanner is not a human eye, and it never sees the ballot the way a human voter does. Determining whether a mark is a vote is a matter of interpretation. This is not so in a DRE system, where it is unambiguous whether a candidate has been selected or not. The statement in ¶67.11 that an optical scan system is "understandable by voters," is incorrect. Voters may think they understand how scanning works, but they are not aware that they can make marks that seem valid to them but will not be counted.

198. The statement in ¶67.11, that voters have no difficulty in telling whether their optical scan ballot has been cast, is misleading. There is a great difference between "cast" and "counted." If "casting" an optical scan ballot means running it through a scanner into a ballot box, a voter can tell whether that has happened. However, there voter has no assurance that the ballot was counted, was counted as she intended, that her ballot will even be in existence at the

[7] Scanners exist which retain a digital image of each ballot, but no such machine is certified in New Jersey.

time a recount is ordered, or that large numbers of forged ballots have not be introduced to swamp and cancel out her vote..

199. A host of insecurities exist in optical scan systems that were never mentioned by Dr. Appel. The list includes manipulations by printers who print the ballots, tampering before the election using invisible inks, hacking by altering the sensitivity of the scanning mechanism, hacking by causing subtle misfeeds of ballots so they will not be counted correctly, collusively feeding multiple ballots into the scanner, ballot-box stuffing[8], altering ballots after they have been cast and literally stealing ballots have been cast. No attention whatsoever has been paid to these risks by Dr, Appel, yet he is willing to conclude that optical scan is preferable to DREs.

200. Section 68 is a summary of Dr. Appel's conclusions. I have already responded to the allegations of ¶¶68.1-68.5. I agree with the conclusions in ¶¶68.6 and 68.7.

201. The ultimate conclusion, expressed in ¶68.8, that the AVC Advantage is too insecure to be used in New Jersey, and that the 2005 law should be "immediately" implemented, is not justified. New Jersey does not face the simple choice of switching voting systems overnight. Florida has gone through the process of using three different voting systems in three successive presidential elections, and has failed to solve its electoral problems. The introduction of a new voting system involves a learning curve for voters and pollworkers, and initially causes more problems than it solves.

202. I have previously explained that precinct-count optical scan is not presently legal in New Jersey, so the sole option presented by Dr. Appel in Section 68 cannot be implemented.

203. The prudent solution is to remediate the problems identified in the AVC Advantage so the risks outlined by Dr. Appel in Section 68 can be prevented.

204. The Appendices give details of various exploits performed by Dr Appel.

205. Paragraph B.1 on p. 146 claims that fraudulent daughterboard firmware can cause the motherboard to reboot, disenfranchising voters, supposedly as described in Section 24 and 26. Those sections do not in fact show that disenfranchisement is possible, merely that it is

[8] Dr. Appel concedes in ¶67.12 that ballot manipulation can occur in optical scan systems.

possible to interfere with or interrupt the normal use of the machine. There is no real difference between and any other malicious mischief that might me performed, such as damaging the ballot face or stuffing chewing gum into the "Cast Vote" button. Both of these would render the machine unusable for a period of time, but would not cause disenfranchisement. The election officials would call for a spare machine to be set up and/or use emergency ballots until the original could be repaired.

206. I agree that possible buffer overflows are bad and should be eliminated. While Dr. Appel claims they can be used to spread fraudulent voter-sealing software vitally, he never performed any experiment to demonstrate that such a thing is even possible on the Advantage. Buffer overflows do not necessarily allow introduction of useful malicious code, and the storage limitations of the Advantage prevent injecting arbitrarily long programs of the type that would be necessary to implement the logic described by Dr. Appel (such as machine learning defenses to parallel testing). Appendix B contains an elaborate description of the Advantage buffer overflow vulnerability, but never explains how it might be used to introduce vote-stealing software.

207. The discussion of compromising voter privacy in Appendix D is more amusing than anything else. It represents no genuine risk. For it to succeed, the observer must know the time each voter cast a ballot to within two seconds (Appel Report, ¶49.6). This is not a simple matter of keeping a stopwatch, as might be supposed, and writing down a sequence of times, even if such behavior could go on unobserved in a polling place. The stopwatch would have to be set to the exact time kept by the machine's internal clock. It is in general impossible to learn this information. In any event, if the risk is regarded as real, the simple expedient of changing the machines clock time by a few seconds at the opening of polls will defeat it.

208. Appendix E lists ways in which Dr. Appel alleges that the Advantage source code violates the 2002 VSS. I have previously explained that the 2002 VSS are not operative in New Jersey and have no legal effect. I have also explained that violation of a voting system guideline does not necessarily mean that the code contains errors, any more than that patrons of a

restaurant would get sick if a cook failed to wash his hands. In fact, Dr. Appel does no identify a single bug that he claims was a result of the claimed violations.

209. Appendix F deals with installation of fraudulent software in the Z80 RAM on Advantage Version 8. In response I observe that tit is always important to prevent people from altering components of voting machines, and this is feasible through administrative mechanisms.

210. Appendix G deals with a feature that is not enabled in New Jersey and is present merely to support Dr. Appel's speculation that "Sequoia engineers do not have a solid understanding of computer security principles." Even assuming the statement to be true, Dr. Appel has not shown that the engineers of the systems he proposes as replacements have any greater understanding of computer security principles.

211. Appendix H suggests that an accidental or deliberate break in a printed cable can cause erroneous results to be printed at the voting machine. First, merely printing erroneous results is only of significance if it is not detected. In this case, the probability of detection is extremely high because the totals reports indicates (1) how many total votes were cast in each office; and (2) how many votes were cast for each individual candidate. The sum of the numbers in (2) must be equal to the number in (1). If the printing is erroneous, it is pure chance for the numbers to add up properly. In any event, the discrepancy between the precinct totals and the results stored on the Results Cartridge will be observed when the cartridge is tabulation at the county clerk's office. Therefore, the risk identified in Appendix H is negligible[9].

212. I agree with the statement in Appendix I, that the undervote warning on Advantage is inadequate. It is not nonexistent, however, and the method of using the office title block to indicate whether or not the office is fully voted, described in ¶I.7-12, is routinely used. I note that the system proposed by Dr. Appel, precinct-count optical scan, does not offer undervote warning at all, so there is no reason why it would be better in this respect.

213. The discussion in Appendix J deals with fleeing voters, which election officials do not regard as a problem of any significance.

[9] Dr. Appel even admits that he at present "cannot say that this is likely to happen." (Report, ¶H.7)

214. The step alleged to be required in ¶J.8 is only necessary if the voter has fled having left an incomplete write-in selection. This situation is so rare as to be statistically negligible. Dr. Appel states that it must be performed for every fleeing voter, which is not true. Even if the situation occurs, the relatively minor inconvenience of feeling for the ENTER button does not disenfranchise the voter and does not expose the voter's choices to scrutiny.

215. Paragraph J.9 complains that the Sequoia AVC Advantage Operator's Manual "prescribes no procedure for fleeing voters." The procedure to be followed for a fleeing voter varies from state to state. In some states, the votes of fleeing voters are voided since the voter did not effect a clear intent to vote (see, e.g., W. Va. Code §3-4A-9(13)(I)). In other states, the vote is to be counted. Therefore, the proper procedure is not determined by the voting system manufacturer, but by the jurisdiction.

216. Dr. Appel fails to note that the fleeing voter situation for optical scan ballots is much worse. Leaving a voted ballot in the polling place without feeding it into the scanner exposes the choices to viewing and alteration not only by pollworkers, but by all the other voters who may enter the polling place to vote.

217. Appendix K claims that a bug in WinEDS causes ballot programming to be "extremely slow." First, Dr. Appel never claims to have measured the time necessary to perform ballot programming. Using file dates on Results cartridges, Dr. Appel computed that only about 8 audio-ballot cartridges per day were made for a particular election in Union County. If that were true, then in a county having "hundreds of voting machines," it would take months to prepare the cartridges. No such behavior has ever been reported. The data in no way implies that ballot programming is made slow by the software, and any such assertion is incorrect.

218. Dr. Appel fails to note that if last-minute changes are made to the ballot in an optical scan jurisdiction, there is no realistic possibility of having new ballots printed in time. DRE systems are much more flexible in this regard than printed-ballot systems. It is odd that Dr. Appel complains of the cost of preparing ballots for an Advantage election, which is vastly lower than the cost of preparing optical scan ballots.

Detecting Malware

219. Dr. Appel repeatedly claims that fraudulent election firmware can successfully evade detection. It cannot. Parallel testing is an effective method of detecting pervasive malware, by which I mean malware that has been installed in a sufficient number of machines that a small random sample of machines with high probability will include one having malware. The theory is that if only a small number of machines are affected, the outcome of the election is unlikely to be altered. To be sure of changing the outcome, a large number of machines must be involved. In any case, Dr. Appel asserts that viral spread is possible, in which case the number of affected machines would continue to increase until all of them have the virus[10].

220. In parallel testing, inspectors are empowered to visit polling locations on Election Day as the polls are being opened, and commandeer and cordon off a voting machine in each of a randomly selected sample of locations. That machine is not used by regular voters, but is used by a panel of test voters who vote according to printed scripts so the correct vote totals will be known. Voting occurs throughout the day and the pace and number of test voters is controlled so as to follow the pattern of normal voters. This is easy. A simple expedient is to have a test voter cast a vote each time a regular voter casts a vote on a specific machine. The polls on the machine under test are closed at the normal poll closing time. A printout of totals is obtained and compared with the predetermined totals. If any vote-swapping has occurred, it will be detected. It is impossible to defeat this mechanism if malware is present, since, despite Dr. Appel's assertions, the malware has no way of knowing that the machine is being tested, for the simple reason that the behavior of the test voters is identical to that of real voters.

221. Another method of detecting voting malware is as follows. It is fundamentally a process called checkpointing, in which vote totals are accumulated and recorded on write-once media (such as a write-once DVD) at certain intervals. Normally vote totals are computed once, at the end of the election, and printed out. However, it is possible to compute vote totals after each 5 voters, for example, and record them in the machine (but not print them out or display

[10] Dr. Appel's scenario in ¶6.19 on p. 26 requires installation of the fraudulent firmware "on many machines used in a particular election."

them during the election). We now empower a test team to cast a small number of ballots during the election, five at a time, starting when the public counter is at a multiple of five. The machine will have no way of knowing that it is being tested, so these ballots will be counted as part of the official total when the polls close. To keep them from affecting the outcome of the election, they must be subtracted manually when the election is over. Now suppose that Dr. Appel's hypothetical invisible and "undetectable" vote-stealing software is present in the machine. The machine cannot cheat on the first five ballots, because those might be a test set. The fraud will be detected at the close of polls when the checkpoint totals for the first five ballots are printed out. The machine cannot cheat on the second set of five ballots, either, for the same reason. In fact, the machine can never cheat without being detected, since any such sequence of five ballots might be a test set, and the machine will be caught if it cheats. So much for the "undetectable" claim.

222. I am not aware of any jurisdiction that uses the foregoing method, which would undoubtedly require statutory changes to implement. It is presented to rebut the unsupportable assertion that malware has the magical property of being undetectable, which is one of the primary bases on which Dr. Appel rests his conclusions.

Voting Machine Security in the New Jersey Election Code

223. An exhaustive review of the voting machine provisions of the New Jersey Election Code, §19:48 and §19:53A-3, reveals only two requirements relating to security.

224. §19:48(i) provides that a voting machine "shall be provided with a 'protective counter' or 'protective device' whereby any operation of the machine before or after the election will be detected." It is undeniable that the AVC Advantage possesses the required protective counter.

225. §19:48(j) provides that a voting machine "shall be so equipped with such protective devices as shall prevent the operation of the machine after the polls are closed." Locking, sealing and maintaining physical custody of a voting machine after he polls are closed prevents operation.

226. There are no other specific provisions of New Jersey law relating to voting system security requirements for certification. §19:48-2, which deals with approval of voting systems, contains a general "safety" requirement: "The Secretary of State within a period of thirty days shall examine the machine and shall make and file in the office of the Secretary of State his report of the examination, which report shall state whether in his opinion the kind of machine so examined can be safely used by the voters at elections under the conditions prescribed in this subtitle. If the report states the machine can be so used, it shall be deemed approved, and machines of its kind may be adopted for use at elections as herein provided." The decision to approve rests with the Secretary of State under the statute. "Safely" is not defined, but several states, including Pennsylvania, have a nearly identical provision. It excludes systems that are so insecure as to be easily tampered with under normal conditions of use. It never imposes a requirement of absolute security or complete protection against tampering, which would be impossible to achieve.

227. Numerous sections of the Election Code specify criminal penalties for various acts of intrusion, including, without limitation, §19:32-13 (destroying or removing seals); §19:34-3 (forging ballots); §19:34-5 (interfering with conduct of election); §19:34-6 (tampering with voting booth); §19:34-11 (fraudulent voting, multiple voting, ballot box stuffing); §19:34-17 (plundering ballot box), §19:53A-15 (assorted misdeeds). These represent the intent of the Legislature that criminal statutes be used as a deterrent to security violations.

228. It may be the case that New Jersey should adopt more stringent security criteria for voting system certification. I note, for example, that New Jersey has not adopted either the FEC Guidelines or the Voluntary Voting System Guidelines promulgated by the EAC. The decision to do so or not do so rests, however, with the Legislature.

229. Dr. Appel, however, has substituted his own judgment concerning voting system security for that of the New Jersey Legislature and urges in his report that the Court impose requirements that are not mandated under existing law.

Constitutional Issues

230. Plaintiffs complain that the use in New Jersey of a voting system that exhibits security vulnerabilities violates the right to vote guaranteed by the New Jersey Constitution. I do not take issue with the principle of law that inherent in the right to vote is the right to have one's vote counted. However, every voting system exhibits security vulnerabilities. Therefore, if the presence of security vulnerabilities means that a system is unconstitutional, then New Jersey would be left with no method whatsoever of conducting elections.

231. It is clear, therefore, that perfection cannot be the litmus test for certification or use of a voting system. In fact, the statutory standard articulated in §19-48-1 is sufficient. The determination whether a system comports with statute has been relegated by the legislature to the Secretary of State. It is not to be usurped by Plaintiffs or their expert, or by me. If there is an allegation that the Secretary or her predecessor did not act properly under the statute in certifying voting systems, the statute itself provides a remedy.

232. The test whether a system can safely be used in elections, as required by §19-48-1, is not to be performed in a laboratory, in which an experimenter has unfettered access to a voting machine for an unlimited period of time and can act unobserved, but is to be made in consideration of the environment in which elections are actually conducted, namely under the supervision of a Board of Elections, a Supervisor of Elections and a County Clerk amid a collection of administrative practices designed to deter commission of crimes defined in the Election Code. The Appel Report gives no consideration to use of voting machines in actual practice, but instead focuses on laboratory manipulation.

Optical Scan in New Jersey

233. Dr. Appel states as one of his conclusions that "New Jersey should immediately implement the 2005 law passed by the Legislature, requiring an individual voter-verified record of each vote cast, by adopting precinct-count optical-scan voting equipment" (p. 144). Dr. Appel appears to have assumed, without checking, that the New Jersey Election Code permits voting by precinct-count optical scan. The literal words of the statute provide for later tabulation of

marked ballots by machine, but do not provide for precinct-count systems in which the voter herself inserts the ballot into a scanner.

234. Fundamentally, §19:53A by its literal terms provides for a ballot marking device (referred to as a "voting device"), which the voter may use to mark a ballot card. The ballot card is then handed to an election official, who deposits it in a ballot box. At the close of polls, the ballot box is opened and the ballots may be read by a machine (called "automatic tabulating equipment" in §19:53A-1(a), which "includes apparatus which automatically examines and counts votes recorded on ballot cards, and tabulates the results").

235. In precinct-count optical scan (PCOS) systems, the voter marks a ballot and then herself feeds t into a scanner. The scanner reads the ballot and can alert the voter to the presence of overvotes and undervotes[11].

236. Optical scan systems are in use in New Jersey, but only as central count scanners for tabulation of absentee ballots[12]. Counting of absentee ballots by optical scanning is permitted by §19:57-15.1. Counting of regular ballots by precinct-count optical scanning during the election is not literally permitted by the Election Code. Therefore, Dr. Appel is not correct that New Jersey could adopt precinct-count optical scanning under existing statutes.

237. The Election Code is replete with provisions dealing with paper ballots and other provisions relating to "voting machines." The paper ballot provisions are inconsistent with optical scan ballots. For example, §19:14-4 states that ballots must contain the following instruction: "The only kind of a mark to be made on this ballot in voting shall be a cross x, plus + or check √." Optical scan ballots require the space next to the candidate name to be filled in completely. In particular, plus marks are rarely recognized by optical scan machines as votes. Therefore, the paper ballots specified in the Election Code are not suitable for optical scanning.

238. §19:15-30 states that "Before leaving the booth the voter shall fold his ballot so that no part of the face of it shall be visible and so as to display the face of the numbered coupon,

[11] Overvote warning is required by HAVA. Undervote warning is not required an is in fact rarely used, even if available, because it would result in a large number of ballots being rejected.

[12] An inventory of voting systems in use in New Jersey can be obtained by following the "Voting Equipment and Systems" link on web page http://www.state.nj.us/state/elections/.

and the ballot of such claimant shall remain in his hand until the board shall have decided to receive the same." Optical scan ballots are not folded, for folding would interfere with being able to feed them into a scanning machine.

239. The need for folding paper ballots is apparent from the procedure used to accept a ballot from a voter. §19-15-31ff. provide that the voter "shall then hand the ballot with the coupon undetached to the member of the election board having charge of the ballot box, which member shall call off the number of the ballot and the name of the voter ... the member of the board having charge of the ballot box, without displaying any part of the face of the ballot, shall remove the coupon from the top of the ballot and place the ballot in the box and the coupon on a file string." The ballot must be folded to prevent the board member from seeing the voter's choices. This statute does not allow a voter to feed the ballot into a machine. The board member deposits the ballot into the ballot box.

240. §19:16-2 provides that, upon the close of polls, "The district board shall then proceed forthwith to count the votes for each candidate or proposition and shall complete such count without delay or adjournment.." In a precinct count optical scan system, ballots are tabulated individually as the voters insert them into a scanner. They are not counted by the board as a batch.

241. Similarly, those provisions of the Election Code dealing with voting machines do not allow optical scanning.

242. §19:48-1 allows voting by "voting machines." It is clear from the statutory provisions that an optical scanner cannot qualify as a "voting machine." (It may qualify as "automated tabulating equipment" under §19:53A, as discussed below.)

243. §19:48-1(g) states that a voting machine "shall for use in primary elections be so equipped that the election officials can stop a voter from voting for all candidates except those of the voter's party." The way in which election officials prevent an optical scan voter from voting for a different party is to control the ballot style provided to the voter. That is, a registered

Democrat receives a Democratic ballot. The machine itself is not equipped as required by statute.

244. §19:48-1(h) states that a voting machine "shall correctly register or record and accurately count all votes cast for any and all persons, and for or against any and all questions." §19:48-1(h) states that it "must permit a voter to vote for any person for any office, except delegates and alternates to national party conventions, whether or not nominated as a candidate by any party or organization by providing an opportunity to indicate such names or name." Taken together, these provisions mandate that write-in votes must be correctly registered and recorded by the voting machine. Optical scanners do not read write-in votes and cannot register or record them. An optical scanner is merely capable of telling that a voter has made a mark in a write-in space. It cannot read the name that has been written in by the voter and is thus incapable of satisfying these statutory requirements.

245. §19:48-1(l) states that a voting machine "shall be provided with a model, illustrating the manner of voting on the machine, suitable for the instruction of voters." In optical scan voting, the voter does not vote "on the machine." This provision clearly contemplates only a direct-recording electronic (DRE) machine.

246. §19:48-1 states that "All voting machines used in any election shall be provided with a screen, hood or curtain, which shall be so made and adjusted as to conceal the voter and his action while voting." Optical scanners are not provided with hoods and do not conceal the voter in the act of feeding a ballot. In fact, the voter cannot be so concealed, or it would not be feasible to detect submission of multiple ballots. The voter must remain in view of election officials. Therefore, this provision certainly does not contemplate optical scanners as voting machines.

247. §19:48-1 states that a voting machine "shall also be provided with one device for each party for voting for all the presidential electors of that party by one operation." Optical scanners do not possess any such "device" for each party and thus do not fall within the voting machine provisions of the statute.

248. §19:53A, which deals with ballot cards, specifies a procedure by which the voter may submit a marked ballot: "After the voter has marked his ballot cards, he shall place the ballot card inside the envelope provided for this purpose and return it to the election officer, who shall remove the stub, place it on a file string, and deposit the envelope with the ballot card inside in the ballot box." §19:53A-7(d).

249. The literal words of the statute provide only for central counting: "As soon as the polls have been closed and the last qualified voter has voted, all unused ballot cards shall be placed in a container and sealed for return to the board of elections. The ballot box shall be opened and any write-in votes counted, unless these votes are to be counted by duly appointed bipartisan tabulating teams at the counting center." §19:53A-7(f). Then: "All proceedings at the counting center shall be under the direction of the county board of elections or persons designated by it; there shall always be two persons in charge who shall not be members of the same political party; and all proceedings shall be conducted under the observation of the public, but no persons except those authorized for the purpose shall touch any ballot card or return. All persons who are engaged in processing and counting of the ballots shall be deputized and take an oath that they will faithfully perform their assigned duties. If any ballot card is damaged or defective so that it cannot properly be counted by the automatic tabulating equipment, a true duplicate copy shall be made and substituted for the damaged ballot card." §19:53A-8(b). Therefore, the voting method literally contemplated by §19:53A is central-count scanning.

250. While the Election Code does not literally permit precinct-count optical scan voting, it does allow for paper trails on voting machines. §19:48-1 reads, "By January 1, 2009, each voting machine shall produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and preserved for later use in any manual audit. In the event of a recount of the results of an election, the voter-verified paper record shall be the official tally in that election. A waiver of the provisions of this paragraph shall be granted by the Secretary of State if the technology to

produce a permanent voter-verified paper record for each vote cast is not commercially available."

251. The technology "to produce a permanent voter-verified paper record for each vote cast" that complies with the 15 mandatory provisions of §19:48-1(a)-(o) is presently not commercially available. For example, DRE machines with continuous-roll paper audit trails do not "secure to the voter secrecy in the act of voting," as required by §19:48-1(a).

252. The very idea that an optical scan system is in some way more secure than a DRE system is completely contradicted by logic and experience. In every election cycle, numerous jurisdictions report loss of optical scan ballots. In some cases the loss is permanent – the ballots are never found. In contrast to DRE machines, there is no backup in an optical scan system. If an original ballot is lost or altered, it can never be reconstructed and recounting becomes unreliable except under imposition of strict chain of custody procedures, which virtually no jurisdiction implements. Even chain-of-custody rules do not prevent alteration or tampering by insiders. In contrast to the hypothetical security risks discussed by Dr. Appel, none of which has ever been known to occur during any election, the risks of paper voting are not only well known, but are in evidence in every election cycle.

253. The most recent incident of this type of which I am aware occurred less than a month ago, in a primary election in Palm Beach County, Florida on September 9, 2008. The community of Boynton Beach ran out of official transport bags for optical scan ballots, so election officials used plastic garbage bags in their place. When all the bags were delivered to the county clerk's office, the garbage bags were naturally taken for garbage and were separated from the other ballots. In one race the candidates were separated by less than 200 votes. When a recount was attempted, it was discovered that more than 3000 ballots were missing. After several days, they were supposedly "found," although at this point no one is able to confirm that the found ballots were the ones actually cast by voters. Part of the reason is that more ballots were "found" than had originally been "lost." This problem is endemic to optical scan elections

and is one reason that New Jersey Attorney General in 2007 rejected switching to a paper (optical) ballot system.[13]

CONCLUSIONS

254. Every voting system ever used suffered from security vulnerabilities. This includes ordinary paper ballots, level machines, optical scan systems and DREs, with or without VVPAT. The presence of a security vulnerability, or even multiple vulnerabilities, does not bar use of a voting system, and certainly does not necessarily rise to Constitutional importance.

255. Rather than banning a entire species of voting system (e.g. DRE without VVPAT) or even a specific voting system (e.g., the AVC Advantage), the responsible action is first to determine whether the vulnerabilities can be remediated and then remediate them. If remediation cannot be performed in time for an upcoming election, then administrative measures should be imposed to reduce or eliminate the possibility of exploiting the vulnerabilities. Not only can the vulnerabilities identified in the Report be remediated, but appropriate administrative procedures can be introduced to reduce the possibility of their exploit.

256. The very vulnerabilities identified in the Appel Report are present in the systems Dr. Appel proposes as replacements, namely DREs with VVPAT and optical scan systems.

257. Replacement of a voting system that is widely used in New Jersey is not a trivial matter. Aside from the expense involved, it takes several election cycles for administrators and poll workers to become sufficiently. States that have frequently change their method of voting in response to demands by activists, such as Florida, have experienced further embarrassment rather than benefit.

258. It is useful that Dr. Appel has identified deficiencies and insecurities in various versions of Advantage. There is not doubt these should be remedied. The question is what to do in the meantime, and the alternatives proposed by Dr. Appel, to replace all of the state's voting

[13] See http://www.nj.gov/oag/newsreleases07/pr20070913a.html.

machines, is expensive and Draconian, particularly when far cheaper and less drastic measures would suffice.

259. The overall conclusion of the Report, namely that the Court should order New Jersey to procure and use precinct count optical scanners, is not justified by the by Report, and is illegal under New Jersey law.

260. Each vulnerability identified by Dr. Appel, if exploited, would be detected by parallel testing.

261. Exploiting the vulnerabilities identified by Dr. Appel can be prevented through administrative remediation.

262. Dr. Appel never discusses the numerous fixes present in Advantage 10 that repair deficiencies in Advantage 8 and 9. A far more prudent solution than the one proposed by Dr. Appel would be to upgrade existing Advantage machines to revision 10 and impose administrative remediations to cover the remaining vulnerabilities.

263. The solution professed by Dr. Appel, namely the use of precinct-count optical scan voting, is not among the remedies sought by Plaintiffs in their Complaint. The Complaint insisted that the state should "require a voter verified paper ballot, produced using the 'Mercuri Method'." (The Mercuri Method is the use of DREs with VVPAT.) Apparently Plaintiffs have recognized that DREs with VVPAT suffer from their own problems, vulnerabilities and lack of secrecy, so they now urge a type of relief not originally demanded.

264. The solution proposed by Plaintiffs, namely to scrap all of the state's existing voting machines and install precinct-count optical scan, is extreme and unnecessary because far less drastic remediation is feasible. Furthermore, this very proposal was implemented in Florida and has not led to success in that state.

Executed on September 30, 2008, in Pittsburgh, PA.

Michael Ian Shamos

Michael Ian Shamos, Ph.D., J.D.