



## 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<sup>1</sup>. 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.

---

<sup>1</sup> 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 150<sup>th</sup> 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 20<sup>th</sup> 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.

