FRANK ASKIN, Esq.
PENNY M. VENETIS, Esq.
RUTGERS CONSTITUTIONAL LITIGATION CLINIC
123 Washington Street
Newark, New Jersey 07102
(973) 353-5687
Attorneys for Plaintiffs

	SUPERIOR COURT
Assemblyman Reed Gusciora, Stephanie Harris,	LAW DIVISION
Coalition for Peace Action, and	MERCER COUNTY
New Jersey Peace Action,	
Plaintiffs,	
v.	
	Docket No.
	MER-L-2691-04
James E. McGreevey, Governor of the State	
of New Jersey (in his official capacity)	
and Peter C. Harvey, Attorney General of	CIVIL ACTION
the State of New Jersey (in his official	
capacity),	
Defendants.	

CERTIFICATION OF APRIL 16, 2008

ANDREW W. APPEL, being of full age, hereby certifies:

1. I am a Professor of Computer Science at Princeton University, and a resident of Princeton Township, Mercer County, New Jersey. I received a bachelor’s degree in physics, *summa cum laude,* from Princeton University in 1981, and a Ph.D. in computer science from Carnegie Mellon University in 1985. I have been on the faculty of

Princeton University since 1986. I am serving as an expert witness in this case.

2. I have served as an expert witness in this case since its inception. This Court recognized and qualified me as an expert in 2006, when I testified at trial concerning the feasibility of upgrading Sequoia AVC Advantage voting machines in time to meet a deadline of January 1, 2008.

3. I submit this certification in support of Plaintiffs' request that counties turn over Sequoia DREs that failed to accurately count the number of voters and/or the number of votes cast in the primary election of February 5, 2008, as well as other materials that will help us to analyze and understand the DREs.

4. I have been retained, along with my colleague Professor Edward W. Felten, by the Plaintiffs to analyze the security of New Jersey's DREs and to determine,

   1. conditions under which they can be tampered with to report incorrect or fraudulent vote totals; and
   2. conditions under which, even in the absence of tampering, these machines report incorrect vote totals.

5. I am working pro bono on this case, as is Professor Felten. Since I have a strong interest in the integrity of elections in New Jersey and elsewhere, I have spent

many hundreds of hours over the past four years studying election equipment and procedures and reporting on the results of my investigations. Professor Felten and our students have also spent many hours pro bono on these studies.

6. There are four different kinds of questions that can be answered by an examination of the voting machines and their software.

- First, do the machines accurately count and report the votes in all circumstances?
- Second, can a person cause the machines to fraudulently misreport votes given if that person has physical access to the machines?
- Third, can a person cause the machines to fraudulently misreport votes even if that person has no physical access to the machines?
- Fourth, what really happened in the primary election of February 5th, and does the miscount exhibited by Sequoia AVC Advantage machines on that date imply that they will miscount votes in other circumstances?

7. Plaintiffs’ counsel issued subpoenas requesting DREs, DRE components, manuals, and other materials that I believe are critical to answering the questions listed in

paragraph 6. Plaintiffs' counsel issued the subpoenas after consulting with me and Professor Felten to determine exactly what we would need to perform this analysis.

8. The subpoenas do not request any superfluous information or materials. I wish to make clear to the court that the materials requested in the subpoena will be examined under the most confidential conditions. I will discuss these confidential conditions below. Now I will discuss in detail the reasons why I need to review all of the items that the Plaintiffs request.

Item 1. Results reports exhibiting discrepancy. Needed to examine the causes of the erroneous results reports printed by Sequoia AVC Advantage voting machines in the February 2008 presidential primary.

Item 2. Voting machine that produced erroneous report. We need this in order to reconstruct and replay sequences of that could cause erroneous reports; and to examine the internal mechanism and software of the machine to determine under what circumstances the machine can be induced to produce erroneous or fraudulent vote totals.

Item 3. Voting machine that did not produce erroneous report. We will compare the operation of this machine, and the internal mechanism and software of this machine, with the erroneous machine. This will help us to determine whether flaws exist on all AVC Advantage machines, or just those that exhibited the discrepancy.

Item 4. Source code. We need this for several reasons, which I will explain in more detail below.

Item 5. Ballot cartridges from erroneous machines. We need this for two reasons: first, to enable us to reconstruct the configuration of the machine at the outset of the primary election; second, because these also contain vote-total results that we can compare with other data such as Result Report tapes.

Item 6. Other ballot cartridges. We need these for two reasons: first, to compare with erroneous ballot cartridges. Second, to construct other test cases to see if erroneous results are produced in election formats not identical to the presidential primary.

Item 7. Ballot Definition Files. We will compare the data on these files to the data contained in Items 5 and 6; and we will use these as a basis for investigations such as those described for item 6.

Item 8. Ballot Cartridge Reader. This equipment is need to access the data in the ballot cartridges.

Item 9. Computer with WinEDS software. Sequoia AVC Advantage machines produce reports in two forms immediately at the close of polls: on a paper printout (Results Report) and in an electronic cartridge (Ballot Cartridge, also known as Results Cartridge). The data in the cartridge is invisible to the pollworkers and witnesses who sign the Results Report at the close of polls, and it may be subject to manipulation (inadvertent or otherwise) by the WinEDS software. We need to examine the interaction of the software with the cartridge. In addition, and equally important, we need use the WinEDS machine to program different election formats to investigate whether erroneous results can be obtained in other than presidential primaries.

Item 10. Copy of AVC Advantage Operating Manual. For two reasons: for our use in operating and examining the machines; and to understand and analyze what happens in actual use by New Jersey election officials who are following the procedures recommended in this manual.

Item 11. Copy of WinEds Operating Manual. For our use in operating and examining the machines; and to understand and analyze what happens in actual use by

New Jersey election officials who are following the procedures recommended in this manual.

Item 12. Copy of poll worker manuals. To understand and analyze what happens in actual use by New Jersey election workers who are following the procedures recommended in these manuals.

Item 13. Service records. To investigate the possibility that the erroneous results are related to the repair, maintenance, and update history of the voting machines.

9. **Why source code is critical.** In order to understand the conditions under which a computer program makes errors, it is necessary to read the computer program. One could in principle reverse-engineer the source code from the contents of the firmware ROM in the machine. In fact, Mr. Edwin B. Smith of Sequoia says exactly this in his Certification of April 7, 2008: "A sophisticated computer expert, given unfettered access to the Voting Machines, could `crack the chip' by decoding the firmware." (Para. 9)[1] Mr. Smith is trying to have it both ways. He says, in effect, that Sequoia cannot release the source code because that is the key to

[1] It should be noted that "crack the chip" is not a term of art in Computer Science; I have never heard this term used; and it is not an accurate description of the reverse engineering process. "Decoding the firmware," the other phrase Mr. Smith uses, is closer to a term of art for this process.

understanding the voting machines;[2] but on the other hand even if they do not release source code, they cannot permit examination of the voting machines because (with effort) someone could reconstruct the source code by reverse-engineering. (In general, this very real possibility means that a person of fraudulent intent can reverse-engineer a voting machine to determine how to make it cheat.)

10. Although we could reverse-engineer the voting-machine software as part of our analysis of its security and accuracy, to do so would require additional effort. It would be entirely artificial and unnecessary to impose this effort on top of an expert study whose main purpose is to examine the reliability of the software. As the Plaintiffs' experts are working pro bono in addition to our regular duties, we cannot afford to undertake this artificial additional reverse-engineering effort. Even the Secretaries of State of California and Ohio, who were compensating the experts they engaged for their services, made sure to provide them with source code to make their work more effective and efficient.

[2] "Review of the source code by a qualified computer programmer would reveal the unique characteristics of the code which cause it to operate the way it does" Smith certification, para. 6.

11. Recent events have shown the need for full examination of the items requested in Plaintiffs' subpoenas. Before 2004, computer scientists could confidently predict, as a matter of basic principles of computer science, that someone with sufficient physical access to a voting machine could replace its software with fraudulent software. However, only more recently have independent computer scientists (not employed by voting machine companies or by testing agencies under contract to those companies) been able to physically examine the internal mechanisms and software of real voting machines. In all such cases, these computer scientists found specific design flaws, thus showing that the machines were much more vulnerable than previously imagined to fraudulent manipulation.

12. I will describe two such cases, concerning specifically the Diebold AccuVote-TS and the Sequoia AVC Edge voting machines. In 2004, academic computer scientists[3] obtained a copy of only some of the source code for a Diebold Accuvote-TS machine (but not the machine itself) and discovered several different kinds of security vulnerabilities, above and beyond those that

[3] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, Analysis of an Electronic Voting System, Proc. IEEE Symposium on Security and Privacy (May, 2004).

could have been predicted from its general design. In 2006, a different group of academic computer scientists[4] (including Professor Felten of Princeton University) obtained unfettered access to a Diebold Accuvote-TS machine (but without source code) and discovered extremely severe vulnerabilities that could not have been predicted from the previously released source code.

13. In 2007 two different groups of academic computer scientists were commissioned by the Secretary of State of California to study Diebold Accuvote machines and their source code. This was done with appropriate nondisclosure agreements to secure the machines and their source code against unauthorized release. This study confirmed the existence of previously found vulnerabilities, and found additional vulnerabilities.

14. Similarly, previously to 2004 computer scientists could say in principle about the Sequoia AVC Edge that a person with physical access to the machine could replace the software. However, in the 2007 study commissioned by the Secretary of State of California, independent computer-science experts studied both the source code and the physical hardware of those machines, and found many

[4] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (September 2006); published in the 2007 USENIX/ACCURATE Electronic Voting Technology workshop, Boston, August 2007.

more design flaws and vulnerabilities. These flaws were far beyond what could have been predicted a priori.

15. Similar studies of these machines and other were commissioned in 2007 by the Secretary of State of Ohio. As in the California studies, independent experts at several universities and other laboratories were given unfettered access to the machines and their source code, with appropriate nondisclosure agreements to secure the machines and their software against unauthorized release. As in the California studies, severe design flaws and security vulnerabilities were found.

16. The design flaws found in the studies commissioned by California and by Ohio were so severe that in 2007 the Secretary of State of each of those States concluded that the machines should be immediately taken out of service. The California SOS decommissioned all the DRE voting machines studied; the Ohio SOS recommend to the Legislature and to the Governor to remove all DRE voting machines from service immediately.

17. The recent studies of voting-machine source code summarized in paragraphs 11-16 above demonstrate that to be able to say with any confidence that a computer program accurately counts votes; or to be able to say with confidence that a computer program is not vulnerable

to fraudulent manipulation, it is absolutely necessary to examine the program in question. This examination must be made by computer scientists in a laboratory equipped for that purpose. The equipment needed for such a thorough examination is that which Plaintiffs requested in their subpoenas to the counties, as well as specialized equipment that we have in our own laboratory.

18. In addition to needing the appropriate materials to examine the DREs, Professor Felten and I need full access to the DREs. It is simply not feasible for Professor Felten and I to examine the DREs ourselves without any support. As I discussed above, both Professor Felten and I have been working on the case pro bono. We have other duties as well; thus we will need assistance from, e.g., colleagues and graduate students.

19. The California and Ohio studies provide good models of what kind of access is necessary for a thorough examination. For example, in the California study, each voting machine was given to two different teams of experts; each team had several members, typically including one or more professors (or PhD scientists outside universities) and several graduate students. All members of the teams signed nondisclosure agreements.

Source code for the machines, and the machines themselves, were provided to the teams.

20. In particular, one of the teams commissioned by the SOS of California to study the source code of a Diebold voting machine consisted of five Princeton graduate students, led by a professor,[5] who performed their study in a secure laboratory in the Computer Science Building of Princeton University.

21. The States of California and Ohio demanded from Sequoia their source for all voting machines in use in those states, as a condition for continued certification of those machines. Sequoia complied with those demands, with the understanding that those states would provide that source code to independent academic experts to study, as I have described.

22. When the State of California sent source code and voting machines for study by experts, it imposed confidentiality requirements regarding the source code and regarding access to the voting machines. For the Court's reference, I attach, as Exhibit A, a copy of the nondisclosure agreement between California and the Princeton team.

[5] Professor David Wagner of the University of California at Berkeley.

23. Computer software is large and complex. A careful study of how software will behave, if that study is to be completed in a limited amount of time, requires a large team. The SOS of California wanted the studies to be completed in a matter of 6 to 8 weeks (preceded by 6 weeks for the investigators to assemble their teams). For each voting machine she commissioned two teams of about 6 people each to study, respectively, the source code and the hardware.

24. It is my opinion that, in order for a study of the Sequoia AVC Advantage to be able to ascertain with confidence whether the machines will operate accurately, a similar size team will be needed, and a similar amount of time.

25. **The New Jersey primary election discrepancies.** In the February 2008 presidential primary in New Jersey, some Sequoia AVC Advantage voting machines indicated more votes cast in the Democratic primary than Democratic voters voting. Other AVC Advantage machines reported more votes cast in the Republican primary than Republican voters voting. In principle this can be caused only be a bug in the computer software inside the machine. What we

do not know is the exact nature of this bug: is the number of votes correct, or the number of voters, or neither? (They cannot both be correct.)

26. After the vote-total discrepancies came to light in February 2008, Sequoia studied the operation of their voting machine, and then issued a memo dated March 4, 2008. This memo indicates one sequence of events by which an AVC Advantage machine can report an erroneous result. Only an examination of the software itself will explain what these paths are, or in what other scenarios they might cause incorrect results, or whether the vote totals are likely to be correct or incorrect.

27. In order to perform such an examination, we would need to operate the machine and to correlate the operation of that machine with the source code, and with the results printed by that machine in the election. For this reason an expert would need the materials requested in Plaintiffs’ Subpoena.

28. I certify that the foregoing statements are true. I am aware that if any statements are willfully false, I will be subject to punishment.

Dated: April 16, 2008	______________________________ Andrew W. Appel
Princeton, New Jersey	