THE RISKS OF COMPUTERIZED ELECTION FRAUD: WHEN WILL CONGRESS RECTIFY A 38-YEAR-OLD PROBLEM?*

After the 2004 presidential election, many Americans expressed concern that the software used in some electronic voting machines had possibly been "rigged" to return a favorable result for the incumbent President Bush.[1] Although most of those who expressed concern believed that no change in the overall outcome of the election would have resulted even if some electronic voting machines were manipulated, they believed that allegations of fraud should nevertheless be investigated.[2] The call for investigations by political figures, including John Kerry,[3] a losing presidential candidate, convinced the investigative arm of the United States Congress—the Government Accountability Office—to investigate the charges of voting irregularities caused by malfunctioning or manipulated electronic voting machines.[4] The concerns that electronic voting machines are highly susceptible to manipulation are not new, and neither are congressional investigations into the vulnerabilities of computerized election systems.

Articles entitled "Vote Tally by Computer Assailed," "12,000 Mysterious San Francisco Votes," and "Those Votes That Weren't Counted" ran in the *San Francisco Chronicle* during November of 1968 and reported allegations that vote-tallying software had been manipulated to produce an outcome for a particular candidate.[5] These early news articles, as well as the reports and studies commissioned by Congress and federal agencies that followed,[6] demonstrate that concerns about the safety and accuracy of election systems utilizing computer software have existed since the systems'

---

* The author would like to thank Professor Wythe Holt, Professor Bryan Fair and Professor Bill Henning, all of The University of Alabama School of Law, for their assistance in writing this Comment. The author would also like to thank Mr. Robert Marshall and Mr. Creighton Miller, both law librarians at The University of Alabama School of Law, for their invaluable help in researching this Comment.

1. *See, e.g.*, Adam Liptak, *Voting Problems in Ohio Set off Alarm*, N.Y. TIMES, Nov. 7, 2004, § 1, at 37; Matthew Marx, *Advocates Propose 11 Ways to Test Vote*, COLUMBUS DISPATCH, Dec. 13, 2004, at A4; Carl Weiser, *Electoral College Today more than Ritual*, CINCINNATI ENQUIRER, Dec. 13, 2004, at A1.

2. Weiser, *supra* note 1; Marx, *supra* note 1; Rick Klein, *Federal Office to Probe Vote Procedures*, BOSTON GLOBE, Nov. 24, 2004, at A1.

3. Weiser, *supra* note 1; Marx, *supra* note 1; Liptak, *supra* note 1.

4. *See* Associated Press, *GAO to Examine U.S. Voting Irregularities*, MSNBC, Nov. 24, 2004, http://www.msnbc.msn.com/id/6575858; Klein, *supra* note 2.

5. *See Vote Tally by Computer Assailed*, S.F. CHRON., Nov. 18, 1968, at 6; Jerry Burns, *12,000 Mysterious San Francisco Votes*, S.F. CHRON., Nov. 22, 1968, at 1; Editorial, *Those Votes That Weren't Counted*, S.F. CHRON., Nov. 25, 1968, at 46.

6. *See, e.g.*, ROY G. SALTMAN, GEN. ACCOUNTING OFFICE, EFFECTIVE USE OF COMPUTING TECHNOLOGY IN VOTE-TALLYING: FINAL PROJECT REPORT (1975), *available at* http://www.eac.gov//bp/docs/NBS_SP_500-30.pdf.

debut in the United States. Because neither the federal government nor state governments have effectively dealt with these concerns over security and accuracy, both expensive litigation and even more expensive statewide and countywide recounts of election totals have followed many "suspicious" election outcomes.[7]

This Comment will first document and explain the various ways in which computers and computer software have been and are currently used in U.S. elections. Next, early problems with the implementation of computers and computer software in elections will be highlighted, followed by detailed examinations of computer scientists' reports on their concerns over the accuracy and security of past and current computerized election systems. Particular attention will be paid to similarities between the concerns of computer scientists in 2004 and 2005 and those voiced by computer scientists over more than three decades ago, as well as to the numerous government-requested studies containing suggestions for preventing, and warnings about the likelihood of, computerized election fraud. Next, lawsuits brought by plaintiffs since the 1970s seeking redress from what they believed were inaccurate election results facilitated by "rigged" computer software will be discussed in detail, with an emphasis on plaintiffs' high burden of proof when such plaintiffs allege computerized election fraud. Then this Comment will discuss the Help America Vote Act of 2002 and the serious inadequacies, both in its requirements and implementation, that are present in the Act in regards to assuring security and accuracy in computerized election systems. Finally, this Comment will address the potential solutions available to Congress through the powers of the Commerce Clause and Article I, Section 4, of the Constitution and Congress's ability to use those powers to restore faith in the accuracy of elections and prevent tampering with computerized election systems.

I. HOW COMPUTERS AND COMPUTER SOFTWARE ARE UTILIZED IN ELECTIONS[8]

Computers and computer software were first used in elections in the 1960s to count and tabulate votes recorded on punch-card ballots.[9] Still commonly used today,[10] voters "record" their votes on punch-cards by

7. *See, e.g.*, Jon Craig, *Coalition to Contest Election Results*, COLUMBUS DISPATCH, Nov. 20, 2004, at B4 (reporting on a coalition that filed a lawsuit contesting Ohio's 2004 presidential election results); Mark Niquette, *Statewide Recount Appears Inevitable*, COLUMBUS DISPATCH, Nov. 16, 2004, at A1.

8. For a general discussion of the various types of voting equipment currently available and their functions, see Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1717-24 (2005).

9. SALTMAN, *supra* note 6, at 10; Roy G. Saltman, *Computerized Voting*, 32 ADVANCES COMPUTERS 255, 257, 266 (1991); *see also* NAT'L CLEARINGHOUSE OF ELECTION ADMIN., FED. ELECTION COMM'N, VOTING SYSTEM STANDARDS: A REPORT ON THE FEASIBILITY OF DEVELOPING VOLUNTARY STANDARDS FOR VOTING EQUIPMENT 10 (1984).

10. Liptak, *supra* note 1.

punching out a perforated hole with a stylus or pen.[11] A computer "ballot box" then "reads" the votes by detecting the holes and recording the number and placement of the holes.[12] Optical scan voting machines are also commonly used today[13] and read marks typically made by pencils on paper ballots and record voters' marked selections.[14]

Direct Record Electronic Voting Systems (DREs) have been used in elections since the 1970s, but they have utilized different user interfaces over the decades.[15] DREs were the intended answer to the problems encountered with punch-card ballots during the 2000 presidential election.[16] DRE voting systems gained widespread usage in the United States prior to the 2004 presidential election, and approximately one third of voters were expected to use them during the 2004 election.[17] The machines themselves were designed to be user-friendly and mimic the familiar design interface of an ATM machine.[18] Today's most common DREs display ballots on computer screens, and voters indicate their selections by touching computer screens.[19] Most DRE models display a "summary screen" that indicates how the DRE will record their votes for each candidate or initiative and require voters to "confirm" their selections by pressing an "accept" button on the screen.[20] The DRE then stores the confirmed votes in both flash memory (like the memory utilized in digital media cards used in digital cameras) and on "internal back-up system[s]" within the DRE.[21]

The vote totals from each of the voting machines are tabulated by computers in either individual precincts or in computers located at central locations within a county or state.[22] Votes cast on DREs are "summarized at precincts, and only grand totals are produced centrally."[23] Punch-card machines vote totals can be counted at precincts or in central locations, as can

---

11. SALTMAN, *supra* note 6, at 10; Saltman, *supra* note 9, at 256.
12. Richard Bergholz, *Experts Game: How Elections Can Be Rigged Via Computer*, L.A. TIMES, July 8, 1969, at 1; Saltman, *supra* note 9, at 256.
13. *See* Michael Powell & Peter Slevin, *Several Factors Contributed to "Lost" Voters in Ohio*, WASH. POST, Dec. 15, 2004, at A1; June Kronholz et al., *Despite Fears, Voters Faced Few Problems, but Very Long Lines*, WALL ST. J., Nov. 3, 2004, at A1.
14. SALTMAN, *supra* note 6, at 12; Saltman, *supra* note 9, at 270-71; *see also* U.S. GEN. ACCOUNTING OFFICE, ELECTIONS: FEDERAL EFFORTS TO IMPROVE SECURITY AND RELIABILITY OF ELECTRONIC VOTING SYSTEMS ARE UNDER WAY, BUT KEY ACTIVITIES NEED TO BE COMPLETED 13 (2005) [hereinafter GAO REPORT], http://www.gao.gov/new.items/d05956.pdf.
15. NAT'L CLEARINGHOUSE OF ELECTION ADMIN., *supra* note 9, at 10; *see also* GAO REPORT, *supra* note 14, at 10.
16. Chris Gaither, *The Race to the White House; Tallying the Woes of Electronic Balloting*, L.A. TIMES, Sept. 24, 2004, at A1.
17. *See id.*; Paul Davidson, *Voting Machine Has Trial by Fire*, USA TODAY, Oct. 29, 2004, at B3; Bill Saporito, *What Could Go Wrong this Time?*, TIME, Nov. 1, 2004, at 36.
18. Gaither, *supra* note 16.
19. Paul Taylor, *Counting on IT at the Polls*, FIN. TIMES, Oct. 20, 2004, at 1; Saltman, *supra* note 9, at 256, 271-73.
20. Taylor, *supra* note 19.
21. *Id.*; *see also* 1 FED. ELECTION COMM'N, VOTING SYSTEM STANDARDS VOLUME I: PERFORMANCE STANDARDS 1-12 to 1-13 (2002) [hereinafter 1 VOTING SYSTEM STANDARDS].
22. 1 VOTING SYSTEM STANDARDS, *supra* note 21.
23. Saltman, *supra* note 9, at 273.

optical scan machines.[24] Controversy over how to secure computerized elections and fears of inadequate security, due to the relative ease with which one can manipulate computer software, have not subsided since the first use of computerized election systems.[25]

II. THE BEGINNINGS OF THE CONTROVERSY OVER COMPUTERIZED ELECTIONS

The first widely reported problems with the use of computers in an election occurred in San Francisco during the 1968 presidential election.[26] A controversy arose after San Francisco election officials attempted to transfer vote totals originally recorded on lever machines to computer-readable cards so that a computer could then compile the election results.[27] The vote totals from the lever machines used in the election were incorrectly recorded onto computer-readable cards, and when officials were ordered to perform a manual recount of the original totals taken from the lever machines, over 12,000 votes had vanished.[28] Public confidence in the use of computers in elections was soundly shaken,[29] and the controversy over the increasing computerization of elections continued into the 1970s.

During a June 1970 election in Los Angeles, California, numerous problems arose when computers were used to compile vote totals from punch-card ballots.[30] First, many of the punch-card ballots were incorrectly printed so that candidates' names did not line up with their intended perforations, and voters were therefore unable to correctly record their intended votes,[31] a problem later repeated in Florida during the 2000 presidential election.[32] Second, an error was discovered in the vote-tallying computer program one hour after the polls closed.[33] Third, another error in the computer programming, which caused the computer to record 700 less votes than had been specified, was later discovered.[34] In 2000, additional issues with punch-card ballots arose when computers failed to read cards that contained "hanging

24. *Id.* at 273-74.
25. SALTMAN, *supra* note 6, at 15; Saltman, *supra* note 9, at 277.
26. *The San Francisco Vote Count—Another Disaster*, S.F. CHRON., Nov. 6, 1968, at 1; *see also* SALTMAN, *supra* note 6, at 15.
27. *The San Francisco Vote Count—Another Disaster*, *supra* note 26.
28. Burns, *supra* note 5.
29. Editorial, *Those Votes that Weren't Counted*, *supra* note 5.
30. SALTMAN, *supra* note 6, at 16 (citing ECON. RESEARCH ASSOC., DETERMINATION OF THE CAUSES OF JUNE 2, 1970 PRIMARY ELECTION PROBLEMS AND RECOMMENDATIONS FOR CORR. (1970)); Phyllis Huggins, *California Controversy over Vote Count Threatens Use of Punched-Card Method*, COMPUTERWORLD, June 10, 1970, at 1; OFFICE OF FED. ELECTIONS, AM. UNIV. INST. OF ELECTION ADMIN. & NAT'L. SCIENTIFIC CORP., A STUDY OF ELECTION DIFFICULTIES IN REPRESENTATIVE AMERICAN JURISDICTIONS, FINAL REPORT 28 (1974); Phyllis Huggins, *The Cal. Elections: A DP Manager's Nightmare*, COMPUTERWORLD, June 17, 1970, at 2; *Who Put the Late in Vote Tabulate?*, DATAMATION, July 15, 1970, at 123; Saltman, *supra* note 9, at 278.
31. SALTMAN, *supra* note 6, at 16; Saltman, *supra* note 9, at 278.
32. *See* Bush v. Gore, 531 U.S. 98, 105 (2000).
33. SALTMAN, *supra* note 6, at 17.
34. *Id.*

chads," as the chads caused the card readers to jam.[35] Finally, "two computer tapes containing all the votes cast for 531 precincts were found to be physically defective and had to be remade from the ballots themselves,"[36] an option which, as will be explained in Part III, is not available for votes recorded on DREs.

In a primary election held in Detroit, in August of 1970, "[t]he vendor of [a] computer program failed to provide the vote-tallying programs to the city election commission fourteen days before the election and provide a certificate of accuracy, as required by regulation."[37] Contrary to Michigan law, not all of the punch-card reading machines were checked for accuracy prior to the primary election, and many of them failed accuracy tests performed just prior to the start of the election.[38] At two polling sites, "the public was not permitted to observe [election] operations, as required by Michigan election law."[39] In another Michigan primary election, held in Redford Township in August of 1972, a computer "program used to count punch-card ballots," which had passed both a logic and accuracy test, was discovered to have an error just prior to the results of the election being certified.[40] "Initial incorrect returns reported that a property tax proposition has been *defeated* by over 1,000 votes while in reality it had *passed* by just over 100 votes."[41] An astute election official caught the discrepancy after he became suspicious of the reported vote totals when one unopposed candidate received "several hundred more votes than another similarly unopposed candidate."[42] A programmer later admitted that the program contained a logic error, which had not been detected during prior logic and accuracy tests.[43] The error during the Redford Township election caused at least one election official to question whether previous elections nationwide had been certified with incorrect results due to programming errors in the vote-tallying software,[44] and all ballots in one precinct were hand-counted to make sure the actual results matched the corrected computer tally.[45]

In 1982, election officials in Elkhart County, Indiana, decided to use a bank's computer to tabulate election results.[46] Bank employees and a vote-

35. *Id.*; *see also Bush*, 531 U.S. at 105.
36. SALTMAN, *supra* note 6, at 17.
37. *Id.* at 19 (citing NAT'L SCIENTIFIC CORP., *supra* note 30, at III-1); Saltman, *supra* note 9, at 279-80.
38. SALTMAN, *supra* note 6, at 19 (citing NAT'L SCIENTIFIC CORP., *supra* note 30, at II-6); Saltman, *supra* note 9, at 279.
39. Saltman, *supra* note 9, at 280.
40. SALTMAN, *supra* note 6, at 20-21.
41. *Id.* at 21 (citing *Tested Vote System Felled by Programmer's Error*, COMPUTERWORLD, Sept. 6, 1972, at 1) (emphasis added); *see also* Saltman, *supra* note 9, at 280.
42. SALTMAN, *supra* note 6, at 21; *see also* Saltman, *supra* note 9, at 280.
43. SALTMAN, *supra* note 6, at 21.
44. *Id.* (citing *Tested Vote System Felled by Programmer's Error*, *supra* note 41, at 1). The Township Clerk was quoted in the same article as stating, "How can you tell that it is not working when every test says it is running perfectly?" *Id.*
45. *Id.*
46. Saltman, *supra* note 9, at 282.

tallying software employee tabulated the votes on the computer while the computer simultaneously continued to run bank operations.[47] Not surprisingly, several races were miscounted, with one error "not discovered until several days after the [election] results were certified."[48] Roy G. Saltman, a computer scientist, later criticized the actions of the Elkhart County election officials, stating:

> It seems clear from the errors of this election that the full implications of computerized voting were not understood by the local election board. The election board seemingly abdicated its authority to bank and vendor employees because of a lack of knowledge by its own personnel. Adequate testing of the system prior to the election was not done, possibly inconsistent with Indiana law and election regulations. Undocumented changes to the system were made during vote tallying. As a result of the errors, lawsuits were filed and the integrity of the entire process was called into question.[49]

III. CONCERNS VOICED BY COMPUTER SCIENTISTS

A. 1960s and 1970s

Along with reports of election malfunctions attributed to faulty programming or "user error," computer scientists in Los Angeles began voicing their concerns during the summer of 1969 about the potential for election results to be intentionally and "secretly altered" through computer programs used in vote-tallying software.[50] The computer scientists (hereinafter referred to as "the 1969 computer scientists") presented no evidence suggesting that any previous election results had in fact been altered, but they were able to demonstrate how the altering of election results could be accomplished.[51] As will be explained in greater detail in Section C, it remains extremely difficult, if not impossible, to prove that computer programs utilized in election systems have actually been manipulated.

In an article published in May of 1970, the 1969 computer scientists detailed the tests they had conducted on a mock punch-card voting system and explained how they were able to alter the results of a mock election.[52] The mock punch-card system that the 1969 computer scientists created included "media conversion" (the transfer of ballot images as recorded by a "card

47. *Id.*
48. *Id.* at 283.
49. *Id.*
50. SALTMAN, *supra* note 6, at 33; *see also* Richard Bergholz, *Experts Game: How Elections Can Be Rigged via Computer*, L.A. TIMES, July 8, 1969, at 1.
51. SALTMAN, *supra* note 6, at 33 (citing Richard Bergholz, *supra* note 50, at 1).
52. James Farmer et al., *Cheating the Vote-Count Systems*, DATAMATION, May 1970, at 76-80.

reader" to a computer-readable medium such as magnetic tape or a disc),[53] "vote counting, and reporting."[54] By inserting a "bias routine" (commonly referred to today as a computer virus) into the operating system program, they were able to alter the correct election totals by 25%.[55] In a second test, they inserted a virus into the vote-counting program's "source code"[56] and again the correct election totals were altered by 25%.[57] A third test, which included the insertion of a virus into the vote-counting program's "object code,"[58] managed to alter the election results by 15%.[59]

As well as demonstrating that vote totals could easily be altered by changing computer programming, the 1969 computer scientists also took pains to detail how, due to inadequate checks and balances in program writing and election-monitoring procedures, a programmer could insert viruses and escape detection.[60] The article noted that "[m]any of the techniques of computer vote fraud require[d] the access of only one person and, at most, an operator and a programmer."[61] The authors emphasized that because computer programs are continuously updated to insert "minor corrections" and to account for changes in election conditions, small amounts of "[c]ode added to a problem program would normally not be identified if added" after the writing of the program had been completed.[62] The article also noted that any changes made to the election system's programs would likely escape the notice of "a casual observer, even if he had extensive data processing background."[63] Because computer programs were often collectively written by several programmers, the programs changed hands several times, causing "operating system[s] [to be] accessible to many" different people, making it "difficult to assign legal responsibility for a routine should fraud be discovered."[64]

Not surprisingly, the concerns expressed by the 1969 computer scientists, prompted Los Angeles to form an "[e]lection [s]ecurity [c]ommittee"

53. *Id.* at 77.
54. *Id.* at 79.
55. *Id.* at 79-80.
56. Source code is defined as "drafted instructions" that are written in "[c]omputer languages . . . similar to conventional language in that they . . . . follow syntactical, punctuational, and formatting requirements" and, like any other written language, can be read and comprehended by those schooled in the language. Steven E. Halpern, *Harmonizing the Convergence of Medium, Expression, and Functionality: A Study of the Speech Interest in Computer Software*, 14 HARV. J.L. & TECH. 139, 142-43 (2000) (footnote omitted).
57. James Farmer et al., *supra* note 52, at 80; *see also* SALTMAN, *supra* note 6, at 34 (discussing the tests performed by the 1969 computer scientists).
58. Object code is "a long combination of 1's and 0's . . . read by the computer, [that] . . . instructs the computer to execute specified tasks." Steven E. Halpern, *supra* note 56, at 144.
59. Farmer et al., *supra* note 52, at 80; *see also* SALTMAN, *supra* note 6, at 34 (discussing the tests performed by the 1969 computer scientists).
60. Farmer et al., *supra* note 52, at 76-80.
61. *Id.* at 77.
62. *Id.* at 79; *see also* SALTMAN, *supra* note 6, at 34 (discussing the article written by the 1969 computer scientists).
63. Farmer et al., *supra* note 52, at 77.
64. *Id.* at 79; *see also* SALTMAN, *supra* note 6, at 34 (discussing the article written by the 1969 computer scientists).

to investigate the allegations,[65] garnering a considerable amount of nationwide attention. The *Los Angeles Times* first reported on the tests performed by the 1969 computer scientists, and stated that programming errors had already caused inaccurate vote tallies in California elections that had only been caught because no votes at all were recorded in favor of popular initiatives.[66] Both the *New York Times* and the *Washington Post* reported on the story, and while both papers noted that no evidence existed that any previous election had been "rigged," their coverage highlighted the tests undertaken by the 1969 computer scientists, which showed that the accuracy and logic tests performed on computerized election systems before and after elections did not discover that the vote-tallying software had been manipulated.[67] The Los Angeles committee's investigation found no evidence of election tampering and stated that "while computer rigging is technically possible, the chances of it [were] extremely remote," and in direct conflict with the assertions made by the 1969 computer scientists in their report, it stated that it "would not be possible without collusion and deliberate intent among several persons having access to election computer[s] and programs."[68]

Once the possibility that computerized elections could be secretly manipulated entered public awareness, discussions about the issues raised and studies conducted by the 1969 computer scientists abounded. In the early 1970s, articles written by computer scientists and the findings of a government-commissioned study discussed the risks involved in utilizing computers in elections and proposed additional security measures to eliminate a majority of the risks of computerized election systems.[69]

In their 1970 article, the 1969 computer scientists called for "extensive research" so that other "potential fraud techniques" could be discovered and safeguards implemented to protect election systems from these techniques.[70] They also proposed several simple safeguards that could have been immediately implemented to reduce the risks of election fraud that their study had already uncovered, which included:

> 1. Examination of the programs for bias routines by a recognized computer professional not associated with either the system design or implementation.

---

65. SALTMAN, *supra* note 6, at 33; *see also Cheating on Vote Tally Eyed*, WASH. POST, July 24, 1969, at F6; *Los Angeles to See if Cheats Can Rig Election Computer*, N.Y. TIMES, July 13, 1969, at 64.

66. *See* Richard Bergholz, *supra* note 12.

67. *See Cheating on Vote Tally Eyed*, *supra* note 65; *Los Angeles to See If Cheats Can Rig Election Computer*, *supra* note 65.

68. SALTMAN, *supra* note 6, at 34 (quoting L.A. COUNTY BD. OF SUPERVISORS, REPORT OF THE L.A. COUNTY ELECTIONS SECURITY COMMISSION (1970)).

69. *See* SALTMAN, *supra* note 6; Farmer et al., *supra* note 52, at 76-80; Robert L. Patrick & Aubrey Dahl, *Voting Systems*, DATAMATION, May 1970, at 81-82.

70. Farmer et al., *supra* note 52, at 80.

> 2. Careful adherence to professionally accepted standards for programs, their documentation, operating procedures, and appropriate system tests.
>
> 3. The monitoring of election counts by computer professionals knowledgeable of fraud routines.
>
> 4. Storing of actual ballots, identified by precinct, for several years following an election. These ballots should be made available to any political party or candidate for partial recount.
>
> 5. Strict access limitation during actual count procedures sufficient to assign responsibility to one person for any error.[71]

The 1969 computer scientists further suggested that "logic and accuracy test[s]" be developed which, when run prior to the start of an election, would "detect any unused code and list all counted program loops."[72] A computer program specialist could then look at the identified pieces of code and determine what purpose, if any, those pieces served, at least somewhat reducing the size of the "haystack" to find the bias routine "needle."[73] The "[i]ncorporation of a full audit trail to provide ballot counts, vote summaries for machine-to-machine and program-to-program comparison" was also suggested.[74] The 1969 computer scientists warned that election fraud accomplished through computers was inevitable because "the men who program and operate [computers] are only human, and subject to human weakness."[75]

Another article, written by two different computer scientists, was published in 1970, containing additional suggestions for increasing computerized election security.[76] The article delved deeper into the computer programming problems brought to light by the 1969 computer scientists and noted that "the vote counting programs use[d] a standard IBM operating system which contain[ed] no provisions to prevent tampering."[77] The article also stated that "there [was] no verification of the operating system prior to the [vote] counting process" and that election counting procedures in one election did not include the disablement of "remote [computer] terminals from which new jobs could be introduced" into the vote-counting software.[78] The authors' most notable suggestion was that the design of the

---

71. *Id.*
72. *Id.*
73. *See infra* note 209 (where statements made by computer scientists in 2003 evidenced the need for a computer program that could decipher poorly written source code).
74. Farmer et al., *supra* note 52, at 80.
75. *Id.*
76. Patrick & Dahl, *supra* note 69, at 81-82.
77. *Id.* at 82.
78. *Id.*

computer "programs and procedures . . . be open to scrutiny so that ignorance does not breed a charge of tampering."[79]

The authors' second suggestion was that "[u]nbroken audit trails . . . be provided so that full accountability and auditability are provided."[80] They stated that "[p]enny accounting techniques should be used to treat each vote as if it [were] precious."[81] Another suggestion included protecting the operating programs of the computers used in elections as vigilantly "as the tally programs [were]."[82] The authors' further suggested that the vote-tallying programs "be read-only," meaning that no changes could be made to the programs at all once they were loaded onto the computers used in an election.[83] As a final suggestion, the authors' noted that election officials and computer programmers should "not let the appearance of mystery pervade."[84]

The impact of the findings made by the 1969 computer scientists and the growing concern over repeated problems encountered with elections when computers were used to tally votes, as detailed in Part II, prompted a United States congressional committee to commission a study in 1974 detailing the risks associated with the increased use of computers in elections and proposing solutions.[85] The Committee asked Roy G. Saltman, the head of the Institute for Computer Sciences and Technology, to write a report detailing his organization's findings[86]—a request he would receive several more times in the following decades.[87] Along with providing detailed ac-

---

79. *Id.*

80. *Id.*

81. *Id.*; *see also* SALTMAN, *supra* note 6, at 35; ROY G. SALTMAN, U.S. DEP'T. OF COMMERCE, ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING 1 (1988).

82. Patrick & Dahl, *supra* note 69, at 82.

83. *Id.*

84. *Id.*

85. SALTMAN, *supra* note 6, at 1. The rationale for commissioning the study and the proposals that were to be included in the study were detailed as follows:

> In recognition of concerns expressed in Congress and by election officials and the public, the Clearinghouse [on Election Administration], through the General Accounting Office, requested that the Institute [for Computer Sciences and Technology] study the use of computers in vote-tallying. . . .
>
> The Institute was specifically asked to "conduct a systems analysis and evaluation of the role of automatic digital processing equipment in the vote-tallying process." Included in the analysis was to be an identification of the hardware, software, and administrative problems that had been encountered; an evaluation, where possible, of the causes of the problems; and an analysis of "methods currently being employed . . . to detect and prevent computer vote fraud." Areas of investigation were to include election system design, training of election officials, ballot accountability, certification and inspection of computer programs, independent audits of election processes, counting center security provisions, and ballot recounts. . . . In addition, the Institute was requested to assess the impact of new technological developments involving computers on the vote-counting process and to provide information on how those developments might be employed and made secure.

Id. at 1-2 (footnotes omitted) (first ellipsis in original).

86. *See id.*

87. *See* SALTMAN, *supra* note 81; *The Importance of Research and Standards in Effective Election Administration: Hearings Before the H. Comm. on Science*, 107th Cong. (2001) (statement of Roy G. Saltman, Consultant on Election Policy and Technology), *available at* http://www.house.gov/science/full/may22/saltman.htm (last visited Feb. 20, 2006); Saltman, *supra* note 9.

counts of the problems encountered with computerized elections prior to 1974,[88] Saltman also suggested the adoption of many of the recommendations put forth by both the 1969 computer scientists and the authors of the article *Voting Systems*.[89]

Saltman also proposed additional protective measures that would guarantee more accurate election results. Saltman considered the software used in vote-tallying to be highly susceptible to tampering.[90] He suggested that "master" copies of software used in election systems be kept separate from "working" copies, with the working copies "compared, bit for bit, against the master copy" for any unexplained alterations before any working copies were actually used in an election.[91] He further suggested that the same comparison between working copies and master copies be performed both immediately prior to an election and immediately after votes totals were computed.[92]

Saltman also believed that any changes to computer programs should be recorded in log books and the logs routinely checked to assure that no one had made any unauthorized changes to the programs.[93] He noted that the programs themselves could be programmed to record the number of times they had been run, and that the number of runs recorded by the program could be checked against a tangible copy kept by programmers.[94] The programs could also be programmed to "automatically report . . . all actions and their times of occurrence that have been taken by operators to change computer operating conditions."[95] Saltman stated that "high-level" programming language, meaning a programming language is largely written with English words, should be utilized when writing vote-tallying programs because it could then be more easily checked for error and would be better understood by election officials,[96] a suggestion repeated by other computer scientists in 2003.[97]

Saltman felt that some of the computerized election system problems that had been reported prior to 1975 could have been prevented had state election officials better performed their managerial and oversight duties.[98] Although some states required vendors of computerized election systems to deposit a copy of the vote-tallying software contained in their machines

88. SALTMAN, *supra* note 6, at 15-32.
89. *Id.* at 35-38; *see also* Part II, *supra*.
90. *Id.* at 50 ("Complex [computer] operating systems . . . are never fully debugged and may contain many routines that could fall prey to tampering," and "no [current] operating system with multiprogramming capability can withstand efforts of a determined penetrator to defeat the operating system's measures to prevent unauthorized alteration.").
91. *Id.* at 51.
92. *Id.*
93. *Id.* at 52-53.
94. SALTMAN, *supra* note 6, at 52.
95. *Id.*
96. *Id.* at 64.
97. *See* Tadayoshi Kohno et al., *Analysis of an Electronic Voting System*, IEEE SYMPOSIUM ON SECURITY AND PRIVACY 2004, Feb. 27, 2004, at 18-19, *available at* http://avirubin.com/vote.pdf.
98. SALTMAN, *supra* note 6, at 59.

with state officials, the programs were not adequately inspected and some states simply relied on programmers' assertions that the programs operated correctly.[99] He noted that election officials had "fail[ed] to develop acceptance procedures for vendors' products and to insure that they are tested sufficiently before acceptance," that there had been a "failure to monitor and control vendors and to limit their activities to what is properly their sphere," and that election workers and officials had not been adequately trained.[100] Saltman emphasized that vendors should be given clearly defined duties during vote-tallying, and that election officials should make sure that vendors did not overstep their assigned duties, and did not allow vendors to perform tasks that were the responsibility of election officials.[101] He felt that if local election officials had their own computer experts readily available, serious conflicts of interest and the potential that computerized vote fraud would go undetected would be greatly decreased.[102]

Saltman also suggested that several states synchronize their requirements for computerized election systems so that they would be able to demand conforming election systems from manufacturers, and noted that manufacturers were unwilling to create multitudes of election systems.[103] In closing, Saltman noted that should states be unwilling or unable "to reform their election practices where needed," then the federal government might provide uniform, nationwide legislation to solve election administration problems.[104]

The Federal Election Commission later ordered a report on state election practices and problems, which was delivered in 1978.[105] The report

---

99. *Id.* at 63.

100. *Id.* at 59; *see infra* notes 145, 153.

101. SALTMAN, *supra* note 6, at 76 (noting that "conflicts of interest may arise" between vendors and election officials and that during one election "local election officials charged that the vendor of the computer program and equipment, who was also operating the equipment on election night, refused to give to the election officials certain computer print-outs, which were clearly election records"). *See infra* text accompanying note 147.

102. *Id.* at 79.

103. *Id.* at 78 (citing COUNCIL OF STATE GOV'TS, POWER TO THE STATES—MOBILIZING PUBLIC TECHNOLOGY xiv-xv (1972)).

104. *Id.* at 88 (citing COUNCIL OF STATE GOV'TS, MODERNIZING ELECTION SYSTEMS 8-9 (1973)). Saltman quoted the report made by the Council of State Governments at length as follows:

> [I]f Congress were willing to involve the Federal government more directly in election administration, a national system would have enormous consequences for the 50 State election systems—not all of which can be anticipated—and would generate stiff resistance from State and local officials. . . . [A] Federal system of election administration could develop if States fail to assume the initiative for insuring procedures that are uniform and convenient to the voters. Even though the administration of elections affects citizens as much as any other government concern, few States have assumed direct responsibility for implementing their own election laws or have established full-time officials to supervise elections as a State activity. . . . [M]ore than 7000 units of local government who conduct elections today . . . are seriously handicapped by a general State reticence in providing money, mandating professional training, or even setting performance standards that would help keep voting opportunities uniform among their own political subdivisions. . . .

Id. (footnote omitted); *see infra* Part V.B.

105. 1 INST. FOR RESEARCH IN PUB. SAFETY, FED. ELECTION COMM'N, AN ANALYSIS OF LAWS AND PROCEDURES GOVERNING CONTESTED ELECTIONS AND RECOUNTS: FINAL REPORT: THE FEDERAL

noted in its introduction that the election results for a number of United States House of Representatives and Senate seats had been appealed to Congress because of the failure of the state election contest procedures to convincingly name election winners.[106] It noted that individuals' votes were diluted by "error[s] in the vote tabulation process" and that "major legislative and administrative change[s]" were needed to assure the validity of elections.[107] The report was highly critical of how election contests were handled by courts, noting:

> Evidence [of the true winner of an election] that might have had a bearing on the case frequently comes out after a contest has been settled.
>
> . . . Contests sometimes also fail to produce accurate outcomes, usually because relevant evidence is not considered. In the most common type of case, discovery opportunities are restricted by procedural delays or because contestants bear unreasonable pre-discovery burdens of proof.
>
> . . . .
>
> . . . The legal system provides no sure method of representing [the] [public] interest.[108]

The report called for states to pass legislation "designed to reduce . . . the excessive burden of proof now placed on contestants."[109]

B. 1980s

In 1985, the *New York Times* published a series of articles in which it was reported that many computer scientists felt computerized election systems were highly susceptible to fraudulent tampering.[110] The articles also discussed several then-pending lawsuits filed by political candidates who

---

PERSPECTIVE (1978).

106. *Id.* at 1 (stating that election contest procedures had "failed miserably, sometimes in ways that have made it forever impossible to ascertain with any degree of certainty at all who really won").

107. *Id.* at 3.

108. *Id.* at 10-11. A detailed discussion of courts' treatment of contested elections is contained in Part IV, *infra*.

109. *Id.* at 12.

110. *See* David Burnam, *Computerized Systems for Voting Seen as Vulnerable to Tampering*, N.Y. TIMES, July 29, 1985, at A1; David Burnam, *Voting by Computer Requires Standards, a U.S. Official Says*, N.Y. TIMES, July 30, 1985, at A17; David Burnam, *Vote by Computer: Some See Problems*, N.Y. TIMES, Aug. 21, 1985, at D20; David Burnam, *U.S. Examines If Computer Used in '84 Election Is Open to Fraud*, N.Y. TIMES, Sept. 24, 1985, at A17; David Burnam, *California Official Investigating Computer Voting System Security*, N.Y. TIMES, Dec. 18, 1985, at B14; *see also* State *ex rel.* Bodine v. Elkart County Election Bd., 466 N.E.2d 773 (Ind. Ct. App. 1984) (illustrating dispute over election results), *vacated*, Estate of Decker v. Farm Credit Serv. of Mid. Am., ACA, 653 N.E.2d 534 (Ind. Ct. App. 1995); Hutchinson v. Miller, 797 F.2d 1279 (4th Cir. 1986) (same).

allegedly lost elections due to the fraudulent manipulation of vote-tallying software.[111] The first article reported on the findings of three computer scientists hired by litigants to scrutinize the software used in vote-tallying, and the reports of two computer scientists who, at the request of the *New York Times*, also looked at the software at issue in the lawsuits.[112] The investigations of all five computer scientists found that the software was susceptible to tampering.[113] One computer scientist claimed that the software used in the voting machines at issue in each of the lawsuits "had been designed in such a way that vote totals could be altered without leaving any sign of tampering."[114] Another stated that the software was so complexly written that "it would take weeks of study to determine" if the program had the ability "to modify election results."[115] The article stated that "[i]n a 1981 report to Congress on the need to develop national voting standards, the Federal Election Commission reported that [vendors of computerized election systems] have 'paid little attention to data quality assessment features.'"[116] It was also reported that although state election officials were certifying the electronic voting machines they received from vendors, no states were "examin[ing] the computer programs used to instruct the equipment how to count the votes."[117]

The second *New York Times* article reported that "the state Democratic Party" of California had asked then "President Reagan and Congress to enact legislation aimed at establishing the mandatory inspection and certification of all computerized election systems."[118] The third article in the series reported that the computer scientists believed that no performance standards for electronic voting machines had been mandated in part because members of Congress believed that Congress should not "oversee" the use of voting machines.[119] The fourth article in the series reported that the National Security Agency, spurred by the publication of the earlier articles in the series, had decided to investigate "the possible misuse of computers to compile election results," although no later articles reported on the findings of the National Security Agency's investigations.[120]

---

111. *Id.*
112. Burnam, *Computerized Systems for Voting Seen as Vulnerable to Tampering*, *supra* note 110.
113. *Id.*
114. *Id.*
115. *Id.* (quoting TIMES second consultant, Eric K. Clemons, associate professor of Decision Sciences at the Wharton School at the University of Pennsylvania); *see infra* text accompanying note 207 (discussing similar findings by computer scientists in 2003).
116. Burnam, *Computerized Systems for Voting Seen as Vulnerable to Tampering*, *supra* note 110; *see infra* note 207 (discussing similar findings by computer scientists in 2003).
117. Burnam, *Computerized Systems for Voting Seen as Vulnerable to Tampering*, *supra* note 110, at B4.
118. Burnam, *Voting by Computer Requires Standards, a U.S. Official Says*, *supra* note 110. This request was made by Saltman in his 1975 report. *See supra* note 104; *see also infra* note 314.
119. Burnam, *Vote by Computer: Some See Problems*, *supra* note 110.
120. Burnam, *U.S. Examines if Computer Used in '84 Election Is Open to Fraud*, *supra* note 110 (quoting Mike Levin, a public information official for the agency's National Computer Security Center).

In response to the concerns raised by the those four articles, the Federal Election Commission (FEC) published an article in its quarterly *Journal of Election Administration* in which it provided election officials with an overview of the perceived areas of risk for electronic voting machines and offered recommendations on how election officials could reduce the risk of tampering.[121] The article noted that the centralization that occurred when votes were tallied by computers caused fraudulent acts to have greater impact than had previously existed when votes totals were not compiled in central locations.[122] It also acknowledged that computerized election systems "impair[ed] the safeguard of public scrutiny" and "require[d] trust in individual technicians . . . performing arcane technical tasks" because "[f]ew ordinary citizens" understood enough about computer programming to decipher whether the systems were operating correctly.[123] The article also noted that while fraudulent programming or "[o]perator manipulation" were of primary concern, the systems were also vulnerable to "*malicious mischief*"[124] by young computer hackers or "political terrorism."[125] To guard against these recognized hazards, the article suggested that election "[d]ata, and the programs that process the data" should be tracked by chain-of-custody logs, with inspections of both data and programs made each time a different person handled them.[126]

Another FEC publication, published in the fall of 1987, contained a section discussing measures that election officials should undertake to better safeguard their electronic voting systems against tampering.[127] The article noted that "compare programs," which compared copies of a computer program with the original program and identified any changes that had been made, were commercially available and should be utilized by election officials in preparing machines for elections.[128] The article cautioned that computer programmers should not also design electronic voting machines,[129] and recommended that vendors perform employment history and criminal history background checks on all employees.[130] The article further recommended that when repairs to electronic voting machines were necessary, election officials should verify the identity of the employee sent by the vendor to perform the repair work by contacting the vendor.[131]

---

121. *See* William Kimberling, *Secure Against What? An Approach to Computer Security*, 13 FEC J. ELECTION ADMIN. 11, 12 (1986).
122. *Id.* at 11.
123. *Id.* at 12. *See supra* note 99 and accompanying text.
124. *Id.*
125. *Id.*
126. *Id.* at 13. These suggestions were virtually identical to those made in Saltman's 1975 report. See *supra* notes 93-95 and accompanying text for Saltman's voicing of the same concerns in 1975.
127. 3 NAT'L CLEARINGHOUSE ON ELECTION ADMIN., FED. ELECTION COMM'N., COMPUTERIZING ELECTION ADMIN.: IMPLEMENTATION STRATEGIES 41-45 (1987).
128. *Id.* at 41. Saltman made essentially the same suggestion in his 1975 report. *See supra* notes 91-92.
129. SALTMAN, *supra* note 6, at 95.
130. *Id.* at 42.
131. *Id.* at 43.

Also in response to the public stir caused by the 1985 *New York Times* articles, Roy G. Saltman published another report in 1988 on the need for improved safeguards to assure the accuracy and security of computerized elections.[132] In his opening summary statement, Saltman stated that "[w]hile proof of actual computer program manipulation appears to be lacking, documentation conclusively demonstrating otherwise is generally insufficient, due to the manner in which many computerized elections are conducted."[133] Saltman went on to discuss several election contests in which one or more candidates alleged that computerized voting systems had been tampered with in order to orchestrate certain candidates losing the election.[134] Two of those candidates are discussed in the context of their resulting lawsuits in Part IV.[135]

Although either the charges were dropped or the lawsuits dismissed because there was insufficient evidence of wrongdoing in each of the alleged tampering incidents,[136] the facts as reported in the news media and as stated in Saltman's report left lingering doubts that perhaps fraudulent election results were in fact certified.[137] In one incident in which election officials allegedly tampered with the computerized vote totals, the ballots from the disputed election were destroyed by an accused election official sixty days after the election.[138] In another dispute, audit trails, which "should consist of everything from the ballots themselves to the console log being printed by the computer on election night," were incomplete due to several "necessary documents" having been destroyed during the course of an investigation.[139] In one election contest in which a jury never heard the facts of the case due to the court's grant of the defendants' summary judgment motion, a computer expert hired by a losing candidate submitted statements stating that an "undocumented program correction" made by a vendor's technician made it "impossible to know exactly how the . . . program tallied the votes."[140] Saltman's report further noted that tests conducted "[b]etween 1983 and 1987" on computerized election systems in [forty-one] Illinois jurisdictions found "computer program tabulation errors in [eleven]" jurisdictions that likely would have gone undiscovered had Illinois not conducted such extensive testing of its computerized election systems.[141]

Saltman's report also reproduced statements made by computer scientists who had been called upon to give advice on matters raised in the elec-

---

132. SALTMAN, *supra* note 81, at 1.
133. *Id.*
134. *Id.* at 52-86.
135. *See* Bodine v. Elkhart County Election Bd., 788 F.2d 1270 (7th Cir. 1986); *infra* text accompanying notes 258-71; Hutchinson v. Miller, 797 F.2d 1279 (4th Cir. 1986).
136. *See infra* Part IV.
137. Doubts over the accuracy of certified election results were also voiced in 1972. *See supra* notes 41-45 and accompanying text.
138. SALTMAN, *supra* note 81, at 56 (discussing the facts of *Hutchinson*, 797 F.2d 1279).
139. *Id.* at 63 (discussing the facts of the contested Dallas mayoral election in 1985).
140. *Id.* at 67 (discussing the facts of *Bodine*, 788 F.2d 1270).
141. *Id.* at 70.

tion disputes or who had been asked to investigate the allegations.[142] A computer scientist named Michael Shamos stated in a Texas legislative hearing that the computer software used in electronic voting systems was "subject to tampering" which was "relatively easy and invisible."[143] Shamos stated "[t]he memories on which these [election] computers operate[d] [could] easily fit into a shirt pocket and [could] be substituted in seconds," that "election counters" could "be altered" by the insertion of "special" ballot cards, and that "[t]he possibilities for this type of tampering [were] endless, and virtually no detection [was] possible once tabulation ha[d] been completed."[144] Shamos further warned the Texas legislature:

> When one company or a conglomerate of companies supply unauditable software from a central distribution point, or participate directly in ballot setup procedures, there exists the possibility of large-scale tampering with elections. An errant programmer or tainted executive could influence or determine the outcome of a majority of election precincts in the country.[145]

Saltman explained that the difficulties experienced in elections across the country were attributable to:

> (a) lack of audit trails;
>
> (b) poor design of computer programs;
>
> (c) vendor-supplied computer programs that [were] unavailable to the scrutiny of responsible officials;
>
> (d) administrative procedures that [were] incomplete and poorly implemented . . . .[146]

Deficiencies in election officials' knowledge of computers and the inability of election officials to attain enough market leverage to demand better products from vendors led to the "abdication of control over elections to vendors."[147]

---

142. *Id.* at 18.
143. *Id.* at 19.
144. *Id.* These comments are similar to those made by the Hopkins computer scientists in 2003. *See infra* notes 197-201 and accompanying text.
145. *Id.* at 20 (quoting Michael Shamos, computer scientist). The CEO of Diebold stated in a 2003 fund-raising letter to fellow Republican supporters that "his goal was 'helping Ohio deliver its electoral votes to the president,'" raising concerns that employees of the voting machine manufacturer might attempt to sway the outcome of the 2004 presidential election by manipulating the computer programming used in their machines. John H. Fund, *No Doctored DRE*, WALL ST. J., July 27, 2004, at A16. Saltman expressed nearly identical concerns in his 1975 report. *See supra* notes 100-03. The 1969 computer scientists also warned of such risks. *See supra* note 75.
146. SALTMAN, *supra* note 81, at 23.
147. *Id.* at 24. Saltman provided a solution to this problem in his 1975 report. *See supra* text accom-

Saltman noted at several different points in his 1988 report that the advice given in his 1975 report was still pertinent and was not being followed by most election officials.[148] Among his new suggestions, Saltman advised that each state adopt statutes like those enacted in Texas after a 1985 Dallas mayoral election dispute, which required, among other things, that Texas' Secretary of State compare computer programs placed on file in his/her office by vendors with the programs used in electronic voting systems in the state to make sure that the programs matched.[149] Saltman also suggested that the computer safeguards that had been adopted in the banking and accounting industries be utilized for electronic voting systems, and that "votes [be] treated as tangible assets and inherently valuable."[150] As in the banking world, Saltman felt that there should be a "[s]eparation of [d]uties"[151] among many election officials and among employees of electronic voting system vendors so that "no one individual [could] control all key aspects" of an election.[152]

At several points in his report, Saltman criticized lax and "sloppy" election procedures and poor managerial performances by election officials.[153] He stated that election officials should "provide their staffs with the necessary guidance and training to help ensure that errors, waste, and wrongful acts are minimized," and that "[a]ccess to resources and records [should] be limited to authorized individuals, and accountability for the custody and use of resources [should] be assigned and maintained."[154] As suggested in his 1975 report, Saltman again stated that "working copies" of computer programs should be compared with "reference copies" to make sure that no unauthorized or unintentional changes had been made to the programs.[155]

Recognizing that the accuracy of elections depended largely upon the adequacy of state election laws, Saltman stated that "[e]ach [s]tate should examine the adequacy of its laws and regulations to assure their effectiveness in treating problems of accuracy, integrity, and security in computerized vote-tallying," and that Texas' statute on electronic voting should provide a model for other states to follow.[156] Saltman advised states to require certification of all software used in elections, and advised state election officials to examine election software to make sure that it could "carry out its asserted function" and that it "contain[ed] no hidden code."[157] "Complete

---

panying note 103.

148. *See, e.g., id.* at 101.

149. *Id.* at 3; *see also* TEX. ELEC. CODE ANN. § 122.0331 (Vernon 2003) (providing the current version of the Texas statute Saltman referred to in 1988).

150. SALTMAN, *supra* note 81, at 90. The same suggestion was made by computer scientists in 1970. *See supra* text accompanying note 81.

151. *Id.* at 95.

152. *Id.*

153. *See, e.g., id.* at 16.

154. *Id.* at 96; *see also supra* text accompanying notes 101 and 145.

155. *Id.*; *see supra* text accompanying notes 91-92.

156. *Id.* at 106.

157. *Id.* at 108.

documentation" of the "functions" performed by the election software should be provided by vendors, as well as "assurances" that copies of the software later provided by vendors performed no additional functions.[158] The statements and assurances made by the vendors should then be verified by independent persons.[159] Saltman further noted that the software used to run DREs should be carefully scrutinized because "no independent proof can be provided to the voter that the choices have, in fact, been entered correctly"[160] and because "[t]here are no ballots that can be recounted as a check on system correctness."[161]

The release of Saltman's 1988 report spurred the publication of a *New Yorker* article in November of that same year, which took an in-depth look at the risks presented by computerized voting.[162] The article noted that few states required vendors to supply the state with the source code used in the vendors' electronic voting systems and that most election officials had no way of determining if the computer software utilized in computerized election systems was actually producing correct vote tabulations.[163] The article also discussed rampant fraud in the banking and insurance agencies carried out by computer hackers and quoted California's then chief assistant attorney general as saying that it was only a matter of time before someone attempted to steal the presidential election by manipulating the software that ran electronic voting machines and that "[t]here is a real reluctance to concede the gravity of the problem."[164]

C. 1990s

Saltman published an article in the journal *Advances in Computers* in 1991 that repeated many of his earlier suggestions for improvement of computerized elections and criticized the 1990 voluntary computerized election standards published by the Federal Election Commission's National Clearinghouse on Election Administration.[165] In his introduction, Saltman stated that "some administrative difficulties with computerized voting" in the last twenty-one years had resulted in "a proportional lack of confidence in the specific results produced" by computerized elections.[166] Saltman noted that both "persons involved with the electoral process as well as . . . journalists and computer-literate lay individuals concerned about the socially responsible use of [computerized voting] machines" had repeatedly expressed their

158. *Id.*
159. *Id.* at 109.
160. *Id.* at 40.
161. *Id.* at 109. *See* text accompanying note 36.
162. Ronnie Dugger, *Annals of Democracy: Counting Votes*, NEW YORKER, Nov. 7, 1988, at 40.
163. *Id.* at 42; *see also supra* notes 98, 147, 153, and accompanying text (discussing how earlier computer scientists expressed similar concerns).
164. *Id.* at 44; *see also supra* note 75 and accompanying text.
165. Saltman, *supra* note 9, at 300.
166. *Id.* at 256.

concerns during the 1980s.[167] Saltman recognized that "[e]ven if elections are honest, public perception that they are dishonest may be just as detrimental to the progress of democratic government," and noted a lack of "[p]ublic confidence . . . . has been prominent ever since computerized voting began in the mid-1960s, and it remains the issue today."[168]

Saltman commented on several problems with DREs, noting the machines do not have "real audit trail[s]," DREs "are not designed to retain individual voter-choice sets,"[169] and that the "data-entry section," or recordation of voter choice, "must be exactly correct and it must be trusted."[170] Responding to suggestions that DREs produce voter "printout[s] stating how the voter voted" to allay fears that DREs could be programmed to wrongly record votes, Saltman stated "[t]his printout may be incorrect; the voter may be told on the printout how his or her votes were cast, but the data-entry logic may be designed to cast the votes in some other way. Unless the internal logic is known to be correct, the truth of the printout cannot be known."[171] Saltman further noted that "[a] statistical verification of the correctness of a DRE machine is not easy" because "the input to the data-entry section is from human action, and to verify its operation, considerable human effort would be required, or a mechanical replacement of the human action would need to be used."[172]

Saltman also discussed problems that occurred when votes were tabulated at either individual precincts or in central locations.[173] Saltman explained that precinct-count systems required the programming of several voting machines at each location, and most of these voting "machines receive their programs on removable memories that were programmed from a central machine."[174] He cautioned that "[t]here must be certain security concerns in delivering the machines to remote or unpoliced locations where the machines might be subject to tampering."[175] Because vote tabulation on central-count systems typically involved only one or two machines, it was "fundamentally important that the counting program" installed on the machine "be correct and that the ballot-reading process be accurate."[176] Saltman then explained that vote-tallying software could contain "hidden code" that could "cause the reporting of election results that are incorrect."[177]

---

167. *Id.* (referencing several newspaper articles from the late 1980s).
168. *Id.* at 257.
169. *Id.* at 272.
170. *Id.* at 273.
171. *Id.*
172. *Id.*
173. *Id.* at 274.
174. *Id.*
175. *Id.*; *see also supra* text accompanying notes 143-44 and accompanying text for similar concerns expressed by Michael Shamos, illustrating concerns similar to those voiced by the Hopkins computer scientists in 2003. *See infra* notes 202-06.
176. Saltman, *supra* note 9, at 274.
177. *Id.* at 277; *see also supra* text accompanying notes 72 and 96 for expressions of the same concerns by computer scientists as much as two decades earlier.

In the conclusion to his 1991 article, Saltman stated that the "public concern [expressed in the 1980s] over the integrity of computerized voting was a replay of the situation that occurred in the late 1960s and early 1970s."[178] Saltman expressed doubts that electronic voting security problems would be corrected in the future due to the failure of state and local governments to implement recommendations included in previous reports and predicted that the election results of jurisdictions utilizing electronic voting systems would continue to be questioned in the future.[179] Saltman concluded that implementing nationally uniform, mandatory election standards could go a long way towards assuring that elections were accurate.[180]

D. 2000s

In 2002, the National Bureau of Standards and Technology published an updated version of voluntary voting systems standards that it had first published in 1990.[181] The report claimed that, as of the date of its publication in April of 2002, "over two-thirds of the States have adopted the Standards in whole or in part."[182] The standards included both qualification testing and certification testing of voting systems.[183] Qualification testing was to be conducted by "Independent Test Authorities" who had been "certified by the National Association of State Election Directors" as capable of adequately testing voting systems.[184] Qualification testing under the standards consisted of determining whether a voting system met "the requirements of the Standards and perform[ed] according to the vendor's specifications for the system" by examining, among other components, software utilized in the machines, quality assurance mechanisms put in place by manufacturers, and performance testing.[185] Once a voting system passed qualification testing, it was assigned a "Qualification Number" and no further qualification tests were performed unless modifications were made to the voting systems by vendors.[186] Certification testing, on the other hand, was to be solely "performed by individual states, with or without the assistance of outside con-

178. Saltman, *supra* note 9, at 301.
179. *Id.* at 302. As an example, Saltman stated that "some very unexpected and unusual voting patterns were reported" in the results of an election "for the U.S. Senate in Florida in 1988," but that "the questions raised in [the] senatorial contest about possible computer-program errors will never be answered with any confidence" because Florida law did not require the "partial manual recount" of ballots or the "review of computer programs used for vote tallying." *Id.* at 302 (citations omitted). Saltman also expressed concern that, because questions concerning the accuracy of the tallies could not be answered, Florida voters would doubt the accuracy of the results reported by their computerized election systems "for the foreseeable future." *Id.*
180. *Id.* at 303. *See supra* note 104 and accompanying text.
181. 1 VOTING SYSTEM STANDARDS, *supra* note 21, at 1-8.
182. *Id.* at 1-9.
183. *See id.*
184. *Id.* at 1-14.
185. *Id.*
186. *Id.*

sultants."[187] It was noted that states "typically rel[ied] on information contained in documentation provided by the vendor."[188]

The publication contained numerous provisions advising election officials on how to assure the security and accuracy of the voting systems, many of which had been suggested previously by computer scientists, such as a provision stating a voting system should "[r]ecord and report the date and time of normal and abnormal events"[189] and vote recording and tabulation software should be submitted to "code inspection."[190] The publication also stated that vendors should "[i]dentify each person to whom access is granted, and the specific functions and data to which each person holds authorized access."[191] Absent from the standards, however, were previous FEC suggestions that "compare programs" be used to validate copies of computer programs prior to their use in electronic voting machines. Saltman's suggestions that "working copies" of the election software be checked and maintained were also absent, as well as any standards addressing the need for vendors to conduct background checks prior to allowing employees to work on election software. All of the standards listed in the publication were well-reasoned and followed many suggestions previously made by computer scientists, but without mandatory enforcement of the standards, and with no one checking to ensure that the vendors actually complied with the provisions after their systems passed qualification testing, problems were bound to arise.

In July of 2003, four computer scientists, two employed by John Hopkins University (the Hopkins computer scientists), published a detailed analysis of the source code installed on a DRE manufactured by Diebold that had been "leaked" on the Internet.[192] Before proceeding to dissect the problems found in the specific DRE model manufactured by Diebold, the Hopkins computer scientists stated that their main concern about the widespread usage of DREs turned on the paperless quality of most of them.[193] They argued that if a DRE printed a paper "receipt," which the voter could observe and verify as correct, "the correctness of any voting software no

187. *Id.* at 1-15.

188. *Id.* For Saltman's 1975 explanation of why reliance on vendors' assertions was dangerous, see *supra* notes 99-101 and accompanying text.

189. *Id.* at 2-23. Saltman suggested this safeguard in his 1975 report. *See supra* note 94.

190. *Id.* at 9-127. The 1969 computer scientists suggested that code be inspected in their 1970 article. *See supra* note 71 and accompanying text.

191. *Id.* at 6-97. The FEC made a similar suggestion more than a decade earlier. *See supra* note 131.

192. *See* Kohno et al., *supra* note 97.

193. *Id.* at 3. The authors also stated:

> The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security-relevant flaws, they might be exploitable either by unscrupulous voters or by malicious insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.

Id.

longer matters."[194] If a "discrepancy in the vote tally" did occur, "the paper ballots [would] be available to be recounted."[195]

The Hopkins computer scientists "discovered significant and wide-reaching security vulnerabilities in" Diebold's DRE.[196] The paper proceeded through an explanation of the processes of initializing the DRE, an action performed by election officials, and voting on the machine. The paper explained that with this particular DRE model, voters were given a "*voter card*," which consisted of a "smartcard" (more commonly referred to as a digital media card).[197] A voter would receive a voter card from election officials at a polling precinct, and in order to vote on the DRE, the voter would be required to insert the voter card into the DRE.[198] When the voter confirmed his or her vote choices, the DRE would "cancel" the voter card, which, according to Diebold, would prevent the card from being used again until it was reprogrammed by election officials.[199] Special smartcards, called "*administrator cards*" or "*ender cards*,"[200] would be used by election officials to end the election and instruct the DRE to transfer the votes it recorded "to a removable flash memory card" or a "back-end server" (a computer storage device capable of storing enormous quantities of data) over a cable or telephone Internet connection.[201]

The Hopkins computer scientists noted that the smartcards used both as voter cards and as administrator cards did "not perform any cryptographic operations," and therefore, "there [was] no secure authentication of the smartcard to the voting terminal."[202] This was of particular concern to the Hopkins computer scientists due to the widespread availability of smartcards purchased on the Internet which could be programmed by any savvy computer programmer to allow a voter to vote multiple times, "terminate the election" on a DRE, or "gain access to . . . administrative controls."[203] Also of considerable concern was the storage of the DRE's election counter, which recorded the total number of votes cast on the machine, in a computer file that could easily be located and changed.[204] The Hopkins computer scientists believed that the location of the file was a violation of the voluntary voting standards promulgated by the FEC, which required counters on election machines to be inaccessible to unauthorized persons.[205] The paper also discussed the absence of any security measures when a DRE transferred its recorded election data to a back-end server over Internet

194. *Id.* at 4. Saltman disagreed with this assertion in his 1991 article. *See supra* notes 169-172.
195. Kohno et al., *supra* note 97, at 4.
196. *Id.* at 4.
197. *Id.* at 7; *see also* GAO REPORT, *supra* note 14, at 12-13.
198. Kohno et al., *supra* note 97, at 7.
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.* at 9 (emphasis omitted).
203. *Id.* at 11.
204. *Id.* These concerns were similar to those voiced by Shamos in the 1980s and Saltman in 1991. *See supra* text accompanying notes 143-44, 175.
205. *Id.* (citing 1 VOTING SYSTEM STANDARDS, *supra* note 21, at 2-33).

recorded election data to a back-end server over Internet connections and hypothesized that election data could be intercepted by employees of Internet service providers or telephone companies.[206]

Perhaps the most troubling finding made by the Hopkins computer scientists, but certainly not the most surprising, given the identical warnings made by earlier computer scientists,[207] was the state of the source code used to program Diebold's DREs. The source code was so poorly written "that any sort of comprehensive, top-to-bottom code review would be nearly impossible."[208] The authors next noted that the inability to effectively review the source code meant that "the chances that bugs exist in the code" were increased and "also implie[d] that any of the [programmers] could insert a malicious backdoor into the system without necessarily being caught."[209] The Hopkins computer scientists "believe[d] that an appropriate level of programming discipline for a[n] [election machine] . . . was not maintained" and that there "appear[ed] to have been little quality control in the process."[210]

Not surprisingly, the Hopkins computer scientists' publication caused quite a stir. Diebold published a rebuttal to the charges leveled against its DREs on the Internet,[211] where it asserted that its DREs were "certified by the National Association of State Election Directors"[212] and noted that election "insiders" could potentially "undermine *any* voting system."[213] Despite Diebold's damage-control efforts, its reputation had already been tarnished. The Hopkins computer scientists published a response to Diebold's attempt to dismiss concerns about its DREs and noted that Diebold did not provide any counter-arguments to several of the scientists' security concerns.[214]

In response to the DRE security concerns highlighted by the Hopkins computer scientists, in August of 2003, the state of Maryland hired an independent team to conduct a review of the Diebold DREs that Maryland had purchased and intended to use in the March 2004 presidential primary.[215] The independent reviewers concluded that "[t]he State of Maryland election system (comprising technical, operational, and procedural components) . . . contain[ed] considerable security risks that [could] cause moderate to severe disruption in an election."[216] The independent reviewers also agreed with

206. *Id.* at 17.
207. *See supra* text accompanying notes 96, 114-15.
208. Kohno et al., *supra* note 97, at 20.
209. *Id.* The 1969 computer scientists expressed similar concerns that just one person could cause the inaccurate tallying of vote totals by manipulating software. *See supra* notes 72-75.
210. Kohno et al., *supra* note 97, at 21.
211. DIEBOLD ELECTION SYS., CHECK AND BALANCES IN ELECTIONS EQUIPMENT AND PROCEDURES PREVENT ALLEGED FRAUD SCENARIOS (2003), http://www.diebold.com/checksandbalances.pdf.
212. *Id.* at 1.
213. *Id.* at 3.
214. Kohno et al., Response to Diebold's Technical Analysis, http://avirubin.com/vote/response.html (last visited Feb. 23, 2006).
215. RABA INNOVATIVE SOLUTION CELL, TRUSTED AGENT REPORT: DIEBOLD ACCUVOTE-TS VOTING SYSTEM (2004), http://www.raba.com/press/TA_Report_AccuVote.pdf.
216. *Id.* at 3.

the Hopkins computer scientists that a paper voter receipt was needed to ensure election fraud did not go unnoticed.[217]

E. The 2004 Presidential Election

Problems with DREs and optical scanners did arise in 2004. The state of California sued Diebold claiming that Diebold had misrepresented the security of its DREs and provided false information regarding the certifications that the machines had undergone; the parties ultimately agreed to settle the lawsuit.[218] Numerous problems with DREs arose during the 2004 presidential election, including one DRE in Ohio which "added 3,893 votes to President Bush's tally in a suburban Columbus precinct that ha[d] only 800 voters."[219] A number of voters reported that DREs displayed votes for candidates that they had not selected on the DREs "summary page."[220] In one Florida county, twenty-five different memory cards that recorded vote totals on Diebold optical scan machines failed, requiring the re-feeding of all of the optical scan ballots.[221] Another memory card failure in North Carolina lost 4,500 votes in one county.[222] Also, an optical scan machine in one Florida county began to "count backwards" after it had recorded 32,000 votes.[223] The number of problems with electronic voting machines that were uncovered after the 2004 presidential election and the enormous media attention the problems received, prompted Congress's Government Accountability Office to launch an investigation.[224]

In September of 2005, an independent commission, led in part by former President Jimmy Carter,[225] released a report in which it detailed the problems that occurred in the 2004 presidential election and proposed various corrective measures that Congress and the states could take to restore Americans' confidence in federal elections.[226] The commission stated, "it is vital to the electoral process that citizens have confidence that voting technologies are registering and tabulating votes accurately."[227] The commission

---

217. *Id.*

218. *See* Greg Lucas, *Settlement in Electronic Voting Lawsuit*, S.F. CHRON., Nov. 11, 2004, at B3; Daniel J. Chacón, *Touch-Screen Voting Machine Maker, State Settle Lawsuit*, SAN DIEGO UNION-TRIB., Nov. 12, 2004, at B2.

219. Liptak, *supra* note 1.

220. *See* Powell & Slevin, *supra* note 13; Kronholz et al., *supra* note 13.

221. *See* Kevin P. Connolly, *Activists Strive to Fix Vote Glitches*, ORLANDO SENTINEL, Dec. 5, 2004, at K1.

222. *See* Mark Schreiner, *Panel Looking at Electronic Voting Getting Some New Clout*, STAR-NEWS (Wilmington, N.C.), Nov. 22, 2004, at B1.

223. *See* Eliot Kleinberg, *Broward Machines Count Backward*, PALM BEACH POST, Nov. 5, 2004, at A29.

224. *See* Rick Klein, *Federal Office to Probe Vote Procedures*, BOSTON GLOBE, Nov. 24, 2004, at A1.

225. David E. Rosenbaum, *Voting Panel Will Propose New Calendar for Primaries*, N.Y. TIMES, Sept. 19, 2005, at A16.

226. COMM. ON FED. ELECTION REFORM, BUILDING CONFIDENCE IN U.S. ELECTIONS (2005), http://www.american.edu/ia/cfer/report/full_report.pdf.

227. *Id.* at 25.

also argued that "Congress should pass a law requiring that all voting machines be equipped with a voter-verifiable paper audit trail"[228] but went on to note that simply requiring a paper receipt would not provide adequate protection.[229]

The commission further suggested that voting machines be audited to assure the vote tallies they reported were in fact accurate, noting that such audits "would encourage both suppliers and election officials to effectively maintain voting machines."[230] Rewording the pleas made by computer scientists for decades, the commission recommended that "[s]tate and local election authorities should publicly test all types of voting machines before, during, and after Election Day and allow public observation of zero machine counts at the start of Election Day and the machine certification process."[231] The commission further noted that "[t]he greater threat" to electronic voting machines came "from insiders who have direct access to the machines" and such insiders could reprogram computer software to return erroneous election results.[232]

> There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it. . . .
>
> . . . [T]he inside process of programming DREs should be open to scrutiny by candidates, their supporters, independent experts, and other interested citizens . . . so that the public will have confidence in the machines.[233]

Instead of calling for voting machine source code to be available to the public, the commission suggested that all voting machine manufacturers "escrow" their source code "with the National Institute of Standards and Technology (NIST)."[234] The escrowed source code would then be made available only to "qualified individuals" such as computer science experts employed by universities or political candidates.[235] The computer science experts would be free to "disclose security flaws or vulnerabilities in the voting system software," but they could not make the source code itself public.[236] The commission recommended that any manufacturer that refused

228. *Id.* at 27.
229. *See id.* at 28. The Commission's determination mirrored that of Saltman. *See supra* notes 168-72.
230. COMM. ON FED. ELECTION REFORM, *supra* note 226, at 28.
231. *Id.*; *see also supra* notes 79, 84.
232. COMM. ON FED. ELECTION REFORM, *supra* note 226, at 28.
233. *Id.* For similar expressions of concern, see *supra* notes 100-102 and 205.
234. COMM. ON FED. ELECTION REFORM, *supra* note 226, at 29.
235. *Id.*
236. *Id.*

to place its voting machine source code in escrow not be allowed to sell its voting machines.[237] The commission also noted that "[w]hen voting machines are tested for certification, a digital fingerprint . . . of their software is often sent to NIST," making it easy for "local jurisdiction[s] [to] compare the software on [voting] machines to" that held in escrow.[238] Local jurisdictions could then assure themselves that no changes had been made to voting machine software after the voting machines received certification.[239] The commission encouraged states to conduct more rigorous testing of voting machines than that conducted by NIST during certification, noting "[w]hen California conducted a mock election with new voting machines in July 2005, it found unacceptable rates of malfunctions that were not apparent in lab tests."[240]

Recognizing that no amount of regulation will dissuade those wishing to illegally change the outcome of elections unless federal and state governments prosecuted those who engaged in election fraud and other election crimes, the commission urged both the Department of Justice and state attorney generals to "prosecute election-related fraud" and report the number of such prosecutions in reports every two years.[241] The commission further criticized the state election administration practices of many states for failing to "allow independent observers to be present during crucial parts of the [election] process, such as the testing of voting equipment or the transmission of results" and noted that "[t]his limits transparency and public confidence in the election process."[242]

The Government Accountability Office also issued a report in September of 2005.[243] The report proved to be a huge disappointment, as it merely synthesized the findings of a multitude of computer scientists.[244] The only essentially new fact contained in the report was that "[o]nly [thirteen] states currently require their systems to be tested against . . . federal [voting] standards by independent testing authorities and certified by the National Association of State Election Directors."[245]

The reports and studies detailed thus far in this Comment represent a small number of the reports and studies on electronic voting security that

---

237. *Id.*

238. *Id.*

239. *Id.* Saltman made similar suggestions in his 1975 report. *See supra* text accompanying notes 90-92.

240. COMM. ON FED. ELECTION REFORM, *supra* note 226, at 29. The commission further suggested that "[l]ocal jurisdictions . . . restrict access to voting equipment and document all access, as well as all changes to computer hardware or software." *Id.* at 30.

241. *Id.* at 45 ("Investigation and prosecution of election fraud should include those acts committed by individuals, including election officials, poll workers, volunteers, challengers or other nonvoters associated with the administration of elections, and not just fraud by voters.").

242. *Id.* at 65.

243. GAO REPORT, *supra* note 14.

244. *Id.* at 22-42.

245. *Id.* at 17. The states that required such certification include Idaho, Wyoming, Colorado, Utah, Michigan, Maine, Delaware, Maryland, South Carolina, North Carolina, South Dakota, Louisiana, and Connecticut. *Id.* at 18.

are widely available. That solutions to electronic voting security issues exist is easily discernible from these studies and reports. The studies and reports discussed in this Comment show that Congress has been aware of security issues since as early as 1975. Not only has Congress failed to pass legislation to force states and manufacturers of voting machines to correct potential electronic voting security flaws, it has also failed to provide courts with an effective means by which to review election results when electronic voting fraud is alleged.

IV. COURTS' REACTIONS TO VOTING MACHINE MALFUNCTIONS

In the majority of election disputes, when candidates believe they have lost an election due to malfunctioning voting machines, they have filed suit under state statutes that authorize courts to order new elections if a candidate is able to prove that, due to one or more malfunctioning voting machines, enough votes were in doubt to cause the outcome of an election to be undetermined.[246] Voters who believe they have been denied their constitutional right to vote due to their inability to record or select the candidate of their choice because of malfunctioning voting machines have filed complaints in federal courts under federal statutes and have attempted to ground their claims under the Due Process Clause and the Equal Protection Clause of the Fourteenth Amendment.[247] As will be explained below, neither of these avenues has afforded either candidates or voters much protection because they fail to allow voters and candidates opportunities to prove allegations of computerized election fraud.

A. Federal Courts

Federal courts have narrowed the scope of relief that defeated plaintiff/candidates can seek under 42 U.S.C § 1983,[248] by requiring candidates to produce evidence of deliberate conduct on the part of election officials carried out with the intent to deprive candidates of the opportunity to be elected.[249] In the first U.S. Court of Appeals case addressing allegations of

246. *See, e.g.*, Haynes v. Williams, 446 So. 2d 750, 753 (La. Ct. App. 1983) ("[I]f a discrepancy sufficient to change the result of the election between the total votes cast at an election and the votes counted for the candidates in the election occurs as a result of a voting machine malfunction, and an accurate count of the votes cast on the malfunctioning machine cannot be determined by the offering of circumstantial evidence or any other evidence, the court shall order a revote in the precinct where the voting machine malfunctioned, which shall be limited to those persons listed on the poll list as having cast their ballots in person at the polls in the election in which the machine malfunctioned."); White-Battle v. Democratic Party of Va., 323 F. Supp. 2d 696 (E.D. Va. 2004); *see also Developments in the Law—Elections—Postelection Remedies*, 88 HARV. L. REV. 1298, 1299 (1975) ("[T]he two principal means by which postelection relief is afforded: statutorily authorized state election contests, and challenges brought in federal court seeking exercise of equitable jurisdiction to remedy violations of federal statutory or constitutional rights.").

247. *See, e.g.*, Shannon v. Jacobowitz, 394 F.3d 90 (2d Cir. 2005).

248. Commonly known as the Civil Rights Act. 42 U.S.C. § 1983 (2000).

249. *See, e.g.*, Hennings v. Grafton, 523 F.2d 861, 864 (7th Cir. 1975) ("[N]ot every election irregu-

either deliberately caused or unintentional voting machine malfunction, *Hennings v. Grafton*, the Seventh Circuit refused to order new elections.[250] Six Illinois plaintiff voters filed suit under § 1983, claiming that they "were deprived of their constitutionally secured rights to vote and to have their votes accurately recorded."[251] In their complaint, the plaintiffs "alleged inaccurate tabulation of votes and 'arbitrary' action by the . . . chief election official, . . . stemming directly or indirectly from the malfunctioning of electronic voting devices that were being used for the first time."[252] The court noted in its synthesis of the facts that "there was uncontested evidence that a number of the machines failed to record votes properly" but that "no evidence of manipulation was introduced."[253] While acknowledging that the right to vote was in fact constitutionally protected,[254] the court elucidated its determination that it was unable to grant the relief requested by stating:

> [T]he record here shows at most irregularities caused by mechanical or human error and lacking in invidious or fraudulent intent; it does not show conduct which is discriminatory by reason of its effect or inherent nature. Voting device malfunction, the failure of election officials to take statutorily prescribed steps to diminish what was at most a theoretical possibility that the devices might be tampered with, and the refusal of those officials after the election to conduct a retabulation, assuming these events to have occurred, fall far short of constitutional infractions, absent aggravating circumstances of fraud or other willful conduct found not to exist by the District Court and not shown by any evidence offered.[255]

The Seventh Circuit further supported its decision to refuse to order a new election by noting that the "experience and intelligence" of those conducting elections, which were typically "volunteers and recruits," "var[ied] widely" and caused "errors and irregularities" to be "inevitable" and remedies for mistakes made by poll workers were not "constitutional[ly] guaranteed."[256] The Seventh Circuit's skepticism of the "theoretical possibility" that computerized vote tabulations might have been manipulated set the

---

larity. . . will give rise to a constitutional claim and an action under section 1983. . . . Infringements of voting rights found to have risen to a constitutional level include dilution of votes . . . purposeful or systematic discrimination against voters of a certain class . . . and other *willful conduct* which undermines the organic processes by which candidates are elected.") (citations omitted) (emphasis added); *see also supra* notes 107-09 and accompanying text.

250. *Hennings*, 523 F.2d at 863.

251. *Id.*

252. *Id.*

253. *Id.*

254. *Id.* (citing Reynolds v. Sims, 377 U.S. 533, 554 (1964)).

255. *Id.* at 864.

256. *Id.* at 865. *See supra* notes 98-99 and accompanying text (showing how Saltman criticized election officials' incompetence).

tone for several subsequent federal court decisions where plaintiffs raised similar allegations and were denied relief.[257]

In *Bodine*, the Seventh Circuit reaffirmed its decision in *Henning*.[258] On similar facts to *Henning*, the *Bodine* Indiana plaintiffs filed a complaint in federal court under 42 U.S.C. § 1983 in which they alleged that election officials had received a faulty computer program from a supplier of a computerized voting system, and that the election officials had failed to perform any logic and accuracy tests prior to tabulating election ballots.[259] Because the complaint failed to allege that the election officials had engaged in fraud, the Seventh Circuit refused to grant relief, stating "the election officials' actions sound more like incompetence than election fraud."[260] However, even allegations of fraud will not guarantee plaintiff/candidates relief from federal courts.

Due to concerns over federalism and encroachment into predicaments reserved for the legislative branch, federal courts have been extremely reluctant to become involved in election disputes brought to federal court under § 1983 when defeated plaintiff/candidates allege that computerized election fraud took place, as explained at length in the Fourth Circuit case of *Hutchinson v. Miller*.[261] In *Hutchinson*, three defeated candidates, including one incumbent United States House of Representatives candidate, alleged that several election officials had engaged in a conspiracy to fraudulently distort the election totals tabulated in a centralized tabulation computer.[262] One witness' testimony described events he observed in the room housing the tabulation computer that were in sync with descriptions provided by computer scientists as methods of manipulating a vote count,[263] including "manipulati[on] [of] computer toggle switches during the election count" and an employee of the manufacturer of the computerized vote system using a "portable modem" contained in his briefcase.[264] The district court had held that the plaintiffs had not proved a conspiracy existed and that their "only evidence the election was rigged was 'purely speculative . . . mere suspicion.'"[265] The Fourth Circuit, in affirming the district court's holding, ex-

257. *See, e.g.*, Bodine v. Elkhart County Election Bd., 788 F.2d 1270 (7th Cir. 1986); *see also* Ryan v. Bd. of Election Comm'rs of DuPage County, No. 94 C 4, 1994 WL 505412, at *4 (N.D. Ill. Sept. 14, 1994) (where a plaintiff/candidate filed an action in federal court under § 1983, alleging that the computer-vote fraud orchestrated by defendant election officials caused him to lose an election and the court denied relief "[b]ecause plaintiff ha[d] failed to allege that defendants acted with purposeful discriminatory intent to deprive him of access to the ballot").

258. *Bodine*, 788 F.2d at 1272-73.

259. *Id.* at 1270-71.

260. *Id.* at 1272.

261. 797 F.2d 1279 (4th Cir. 1986).

262. *Id.* at 1280-81.

263. *Id.* at 1281; *see also supra* notes 71 and 78 (suggesting that the number of people granted access to vote-tallying computers should be limited during the counting of votes).

264. *Hutchinson*, 797 F.2d at 1281.

265. *Id.* at 1282 (ellipsis in original). Additional evidence suggesting tampering that the court refused to credit was that all of the ballots from the election were destroyed sixty days after the election by one of the accused defendants. *See* SALTMAN, *supra* note 81, at 56; Saltman, *supra* note 9, at 282 ("The destruction of the punch-card ballots made it impossible to verify the outcome of the election through a

pressed a profound reluctance to allow the plaintiffs an opportunity to make their arguments in front of a jury because to allow a jury to pronounce a verdict on the "election results would be inconsistent with proper respect for the role of others whose job it is to canvass the returns and declare a prevailing party."[266] The court also foresaw federal courts being called upon again to review a determination made by a jury.[267] "Principles of separation of powers and federalism . . . dictate that both jury and court avoid th[e] inquiry."[268]

The Fourth Circuit attempted to further justify its determination that plaintiffs should be unable to seek relief in federal courts when computerized election fraud was alleged because "federal courts [were] ill-equipped to monitor the details of elections and resolve factual disputes born of the political process,"[269] an argument which, if believed, would seem to imply that federal courts were "ill-equipped" to make any factual determinations when compliance with state statutes was at issue. The Fourth Circuit also stated that "[e]lections are, regrettably, not always free from error"[270] and, "irregularities . . . are inevitable in elections staffed largely by volunteers."[271]

Federal courts should not be so quick to sidestep issues affecting the fundamental rights of persons to have their votes accurately counted. Acceptance of irregularities as being "inevitable" shows a gross disrespect for the rights of both the candidates who failed to win elections due to irregularities and voters. The Framers' confidence that Congress would assure that fair and accurate elections would take place was obviously misplaced, as Congress refused to correct the potential for electronic voting fraud after being made aware of the problem for more than three decades. Federal courts repeatedly assert that the irregularities alleged by candidate/plaintiffs are best solved by the legislative branches of government, but how many

---

recount . . . .").

266. *Hutchinson*, 797 F.2d at 1286.

267. *Id.*

268. *Id.* In its discussion of the importance of a separation of powers in matters before federal courts involving state election disputes, the Fourth Circuit also stated:

> We thus proceed with awareness that the resolution of particular electoral disputes has been primarily committed to others in our system. The express delegation to Congress and the states of shared responsibility for the legitimation of electoral outcomes and the omission of any constitutional mandate for federal judicial intervention suggests the inadvisability of permitting a § 1983 or civil RICO action to confer upon federal judges and juries "a piece of the political action," no matter what relief is sought. Consideration of the various ways in which these other bodies have regulated and monitored the integrity of elections only confirms our hesitation to consider the disputed details of political contests.
>
> . . . Had the framers wished the federal judiciary to umpire election contests, they could have so provided. Instead, they reposed primary trust in popular representatives and in political correctives.

Id. at 1284.

269. *Id.* at 1286.

270. *Id.*

271. *Id.* at 1287. The Fourth Circuit also partially based its decision to refuse to grant the plaintiffs a trial because the plaintiffs were seeking monetary damages as compensation for the salaries they would have received had they actually been elected. *Id.* at 1279-80, 1287.

decades and how many cases are necessary to make it the job of the federal judiciary to correct problems that both state and federal legislatures have refused to address?

B. State Courts

Over the last three decades, candidates have filed suit under state election contest statutes more frequently than under federal statutes. They have requested that recounts or new elections be conducted by alleging that vote totals were subject to computer tabulation errors or were fraudulently manipulated during computerized vote tallying.[272] Candidates are typically not successful in attaining recounts or new elections when computerized voting machine "irregularities" occur. The Ohio Supreme Court provided a typical example of how state courts address computerized election fraud allegations in *In re Election of November 6, 1990*.[273]

In *In re Election of November 6, 1990*, a candidate in the Ohio's Attorney General election lost the election by "less than one-quarter of one percent," triggering a recount.[274] After the recount took place, the candidate filed suit, claiming, among other things, that during the statewide recount, optical scanning machines used to tabulate ballots in one county were "in such [a state of] disrepair that different machines counted the same ballots differently."[275] He further claimed, "ballots were moved from one optical scanning machine to another until a count was obtained that agreed with earlier tabulations; and that in [one county] the automatic tabulating machine results produced more votes than there were names of voters recorded in the poll books."[276]

Before addressing the specific complaints alleged by the losing candidate, the Ohio Supreme Court set out the test it deemed itself to be bound by prior caselaw to follow.[277] The test "requir[ed] a contestor to prove two facts: (1) that one or more election irregularities occurred, and (2) that the irregularity or irregularities affected enough votes to change or make uncertain the result of the election."[278] The court then stated that it was adopting a clear and convincing burden of proof that must be met by the complaining candidate in that case, as well as all those who contest election results in the

272. *See, e.g.*, Barrera v. Superior Court, 573 P.2d 928 (Ariz. Ct. App. 1977); Enter. Residents Legal Action Against Annexation Comm. v. Brennan, 587 P.2d 658 (Cal. 1978); Bodine v. Elkart County Election Bd., 466 N.E.2d 773 (Ind. Ct. App. 1984); *In re* Election of Nov. 6 for the Office of Attorney Gen. of Ohio, 569 N.E.2d 447 (Ohio 1991); *In re* Bamberg, 524 S.E.2d 400 (S.C. 1999); Palm v. Lesher, 489 S.W.2d 351 (Tex. Civ. App. 1973); Underwood v. County Comm'n of Kanawha County, 349 S.E.2d 443 (W. Va. 1986); Ohio County Comm'n v. Manchin, 301 S.E.2d 183 (W. Va. 1983).

273. 569 N.E.2d 447 (Ohio 1991).

274. *Id.* at 448.

275. *Id.*

276. *Id.*

277. *Id.* at 450.

278. *Id.*

future.[279] The court found that evidence produced by the candidate that a computer program used in each of the optical scanning machines which caused several machines to either record or reject ten "test" ballots differently did not meet the required clear and convincing standard of proof "that an irregularity [had] occurred."[280] In addressing the candidate's evidence that more votes or fewer votes were recorded than voters who signed the precinct poll books, the court did find that the candidate had provided clear and convincing evidence of an irregularity; however, the candidate had not shown that the number of votes in doubt due to this unexplained irregularity were enough to change the outcome of the election.[281]

Given the clear and convincing burden of proof a candidate is required to show, it is evident that the majority of irregularities or fraudulent acts which do occur will go unremedied. Meeting the clear and convincing burden would necessitate a candidate not only locating witnesses able to testify to irregularities or fraudulent acts, but also being able to access the computer software within the machines before the software could be altered and have it inspected by persons knowledgeable in computer programming. Then the candidate would be required to show through expert testimony that any error found did in fact cause a certain number of votes to be uncertain. In light of the preceding statements made by computer scientists, discussed in Part III, that the source code used in electronic voting machines was so complex it would be nearly impossible to find an error or a computer virus intended to throw an election,[282] this burden of proof is virtually impossible to meet.

V. CONGRESS'S POWERS TO ASSURE SAFE AND ACCURATE COMPUTERIZED FEDERAL ELECTIONS

A. The Help America Vote Act

Congress enacted the Help America Vote Act of 2002 (HAVA)[283] in response to the glaring problems with the state voting systems that were placed in a global spotlight in the aftermath of the *Bush v. Gore*[284] elec-

279. *Id.*

280. *Id.* at 459. The court explained the rationale for its holding by stating, "We find that contestor's tests prove no more than . . . that different sensitivity levels of machines will produce greater or fewer numbers of overvotes and undervotes" and that "contestor's tests do not establish that any vote was changed from one candidate to another." *Id.* The court's high evidentiary standard and rationale do not rule out all future claims of programming error causing erroneous election results, as the court left room for an argument to be made by a future contesting candidate that, due to fraudulent or malfunctioning programming, a DRE either did or could have changed a vote from one candidate to another. The contesting candidate would have to provide enough proof to meet the clear and convincing burden, which may be an impossibly high burden of proof given current voting machine regulations and lack of access to the computer programs installed in DREs. *Id.*

281. *Id.* at 462-63.

282. *See supra* notes 96, 113-15, 207-10 and accompanying text.

283. 42 U.S.C. §§ 15301-15545 (Supp. II. 2002).

284. 531 U.S. 98 (2000).

tion.[285] HAVA provides monetary disbursements to states enabling them to improve their voting systems for federal elections.[286] Congress wished to avoid having another federal election challenged due to "hanging chads" from punch card ballots[287] and accordingly, HAVA mandates that each state receiving federal funds for the improvement of its federal voting systems replace all "punch card voting systems or lever voting systems" prior to January 1, 2006.[288] This means that optical scan and DRE voting machines will be virtually universally utilized in federal elections beginning in 2006.

Included in HAVA are mandatory "[v]oting systems standards" that states must follow for voting machines used in federal elections, with the deadline for state compliance also set at January 1, 2006.[289] Showing Congress's evident awareness of at least some of the safeguards computer scientists have proposed, the mandatory standards require voting systems to "produce a permanent paper record" for auditing purposes[290] and also require that "[t]he paper record . . . be available as an official record for any recount . . . [of] any election in which the system is used."[291] Voting systems must also have "a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions."[292] Congress also ordered states to "adopt uniform and nondiscriminatory standards that define what constitutes a vote and what will be counted as a vote for each category of voting system used in" each state.[293]

Congress apparently utilized its constitutional powers to enact mandatory regulations for voting systems by choosing the wording "[e]ach voting system used in an election for *Federal* office *shall meet* the following requirements."[294] Congress appears to have referenced its Article 1, Section 4 power, which gives Congress the power to "make or alter" voting regulations enacted by state legislatures.[295] While Congress clearly has the power to make alterations to state voting regulations for congressional elections, it

285. *See* Martin J. Siegel, *Congressional Power over Presidential Elections: The Constitutionality of the Help America Vote Act Under Article II, Section I*, 28 VT. L. REV. 373 (2004); R. Bradley Griffin, *Gambling With Democracy: The Help America Vote Act and the Failure of the States to Administer Federal Elections*, 82 WASH. U. L.Q. 509 (2004).

286. § 15301.

287. *See Bush*, 531 U.S. at 105 ("Much of the controversy seems to revolve around ballot cards designed to be perforated by a stylus . . . . In some cases a piece of the card—a chad—is hanging, say, by two corners.").

288. § 15302(3)(A); *see also* GAO REPORT, *supra* note 14, at 14.

289. § 15481.

290. *Id.* § 15481(a)(2)(B)(i).

291. *Id.* § 15481(a)(2)(B)(iii).

292. 1 VOTING SYSTEM STANDARDS, *supra* note 21, at 3.4.

293. § 15481(a)(6).

294. § 15481(a) (emphasis added).

295. U.S. CONST. art. I, § 4, cl. 1 ("The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators."). *Compare* Saltman, *supra* note 9, at 260, *with* GAO REPORT, *supra* note 14, at 5-6.

is at least somewhat questionable whether Congress also has the power to issue regulations that will apply to presidential elections as well.[296]

HAVA also established the Election Assistance Commission (EAC),[297] consisting of four members (two from each major political party)[298] to disperse funds to states,[299] conduct studies on ways to improve federal elections,[300] and assemble a board to carry out voluntary certification testing of electronic voting systems.[301] States, however, are not required to have their voting machines tested or certified by any agency prior to their use in federal elections.[302] Although the establishment of the EAC was laudable, Congress failed both to fund the fledgling commission and to establish it within the time parameters set out by HAVA.[303] Given the public outcry that followed the 2000 presidential election, it is surprising that Congress failed to carry out its duties in regards to the implementation of HAVA. Even more surprising is Congress's failure to incorporate more of the safeguards that have been suggested by computer scientists over more than three decades.

In its opening remarks, the Commission on Federal Election Reform (Commission) stated in its 2005 report that "Americans are losing confidence in the fairness of elections" and that HAVA, as then currently written, was not enough to fix the glaring deficiencies observed during the 2004 presidential election.[304] The Commission noted that as of the date of its report's publication, HAVA still had not been fully funded.[305] Among its numerous criticisms of HAVA, the Commission pointed out that the EAC did not have the authority to speak definitively on any of the many mandates the EAC had been entrusted to enforce under HAVA.[306] In perhaps the most shocking revelation, the Commission expressed concern that Congress would not pass much needed amendments to HAVA, noting that "Congress has been reluctant to undertake reform, in part because members fear it could affect their chances of re-election and, when finally pressed by the

296. *See* Siegel, *supra* note 286, at 417-18, 422 (stating that federal courts may be willing to uphold HAVA as constitutional under Article II, Section 1 in the wake of the 2000 election).
297. § 15321; *see also* GAO REPORT, *supra* note 14, at 15.
298. *Id.* § 15323.
299. *Id.* §§ 15322(4), 15401(a).
300. *Id.* § 15322(3).
301. *Id.* §15371.
302. *Id.* § 15371(a)(2).
303. U.S. ELECTION ASSISTANCE COMM'N, FISCAL YEAR 2004 ANN. REP. 3 (2005), *available at* http://www.eac.gov/docs/EAC%20Annual%20Report%20FY04.pdf ("The Commission began operation in January 2004, and overcame numerous challenges, the first and greatest of which was its actual launch. EAC was established 10 months later than required by the Help America Vote Act of 2002 (HAVA), was seriously under funded, and had no offices, equipment, or staff. The total operating budget for Fiscal Year (FY) 2004 was just $1.2 million.").
304. COMM. ON FED. ELECTION REFORM, *supra* note 226, at ii. The commission also stated, "Democracy is endangered when people believe that their votes do not matter or are not counted correctly." *Id.* at 1.
305. *Id.* at 2.
306. *Id.* at 4.

public, Democrats and Republicans have addressed each reform by first asking whether it would help or harm each party's political prospects."[307]

In its 2005 report on electronic voting,[308] the GAO referenced a multitude of studies and papers circulated by computer scientists and election officials which discussed virtually all of the electronic voting security flaws detailed in this Comment.[309] The GAO concluded its report by recommending that the EAC take several actions, which mainly included partnering with another organization to provide information on electronic voting security vulnerabilities to state election officials.[310] The report contained no other suggestions for the improvement of electronic voting security.[311] The report also failed to suggest how the EAC should implement the GAO's recommendations, nor did it discuss where the additional funding the EAC would need to carry out the recommendations would be found.[312] The GAO's report evidenced that at least some current members of Congress are in fact aware of the extent of the electronic voting security problem, but that those Congress members cannot or will not propose any viable solutions to fix the problem.

B. Solutions Available to Congress to Fix a Thirty-Eight-Year-Old Problem

As Roy G. Saltman realized in 1975 and restated in 1991, and as has proved true in the three decades following his 1975 report to Congress, nationwide federal legislation is needed to establish uniform electronic voting security methods.[313] A multitude of options are available to Congress to increase the security of computerized voting systems used in federal elections. Congress could amend HAVA to include more rigorous mandatory voting systems standards. Some members of Congress have proposed amendments that would require all DRE machines to print a paper voter receipt so that if questions about the accuracy of the election results did arise, hard copies demonstrating voters' choices would be available.[314] However, as has been argued by at least one computer scientist,[315] and as should be apparent from arguments made by computer scientists in the past

307. *Id.* at 7.
308. *See* GAO REPORT, *supra* note 14.
309. *Id.* at 22-42.
310. GAO REPORT, *supra* note 14, at 53-54.
311. *Id.* at 56. The EAC understandably balked at having its actions deemed the sole means by which electronic voting security could be improved, yet the GAO responded by stating that "given [the EAC's] leadership role in defining voting system standards, in establishing programs both to accredit laboratories and to certify voting systems, and in acting as a clearinghouse for improvement efforts across the nation, we believe that our focus on EAC is appropriate." *Id.*
312. *See id.* at 54.
313. *See supra* notes 104 and 118 and accompanying text; Saltman, *supra* note 9, at 303.
314. U.S. Representative Rush Holt proposed a bill that would require DREs to print a paper receipt showing how a voter voted. H.R. Res. 550, 109th Cong. (2005), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h550ih.txt.pdf.
315. *See* Saltman, *supra* note 9, at 272-73.

when paper copies of ballots were available, paper receipts will do little to assure that election results are accurately determined if states remain unwilling to make extensive comparisons of paper copies with computer-reported totals.

Congress would best be able to assure the accuracy and security of federal elections if the manufacturers of computerized voting systems were themselves subject to mandatory federal regulations enacted under Congress's Commerce Clause power.[316] The need for mandatory federal standards for electronic voting machines has been recognized for at least two decades as the only truly viable solution to a nationwide problem.[317] Computerized voting systems sold to various state and local election officials are "thing[s] in interstate commerce,"[318] and even under the recent, restrictive interpretations of Congress's Commerce Clause power evidenced in the United States Supreme Court's decisions in *United States v. Lopez*[319] and *United States v. Morrison*,[320] Congress does have the authority to regulate voting systems sold to states. The Supreme Court's reining in of Congress's Commerce Clause power under both *Morrison* and *Lopez* was achieved by limiting Congress's ability to enact laws where commerce was "substantially affected."[321] Neither opinion imposed any additional restrictions on Congress's ability to enact laws affecting things bought and sold through interstate commerce.[322]

Congress has enacted federal regulations applicable only to manufacturers of products in several instances, with an obvious example being the requirement that automobile manufacturers produce cars that achieve a certain minimum number of miles per gallon of gasoline.[323] Were Congress to draft regulations that tracked the suggestions of computer scientists and required manufacturers of computerized voting machines to produce machines that complied with those suggestions made by computer scientists, not only would the accuracy and security of federal elections be drastically improved, but voters and their advocates would have little to justify their complaints. The responsibility for assuring that votes in federal elections are accurately counted would rest with the legislative branch of the federal government, which arguably should have been assuring the accuracy and secu-

316. U.S. CONST. art. I, § 8, cl. 3.

317. *See* Burnam, *Vote by Computer: Some See Problems*, *supra* note 110; Paul Houston, *Computerized Vote Tallies Have Too Many Glitches, Experts Charge Technology*, L.A. TIMES, Dec. 3, 1989, at A45 ("[T]he need for mandatory federal standards because without them, the integrity of elections on highly sophisticated electronic systems cannot be guaranteed . . . ."); Saporito, *What Could Go Wrong This Time?*, *supra* note 17, at 36.

318. United States v. Lopez, 514 U.S. 549, 559 (1995).

319. *Id.*

320. 529 U.S. 598 (2000).

321. *Id.* at 609.

322. *See id.*; *Lopez*, 514 U.S. at 560.

323. *See, e.g.*, 49 U.S.C. §§ 32902, 32904-05 (2000).

rity of federal elections long before now, given the failings of the states to do so.[324]

In HAVA, Congress has already established many of the mechanisms by which the manufacturers of voting systems could be regulated. The EAC has created certification laboratories which are currently available for the voluntary testing of states' electronic voting systems.[325] It would be only a small step, necessitating little, if any, additional federal funds, to require voting systems manufacturers to subject their machines to testing by these independent laboratories. Members of the laboratories could also perform random, on-site inspections of the machines and investigate reports of errors or attempted fraud. Also, if all computerized voting machines were required to conform to identical standards, the accuracy and reliability of the machines would be uniform no matter which types of voting machines states chose to use for federal elections, thereby addressing equal protection concerns.[326]

Federal courts have been willing to hold the manufacturers of electronic voting systems accountable for the performance of their machines in the past, as evidenced by the Third Circuit decision in *Montgomery County v. Microvote Corp.*[327] There, the Third Circuit upheld a jury's finding that the poor performance of Microvote's DREs in one Pennsylvania county constituted a breach of the implied warranties of merchantability and fitness for a particular purpose.[328] Rather than forcing state and local governments to resort to legal remedies provided under the Uniform Commercial Code, Congress could virtually eradicate the need for these types of actions by requiring manufacturers to comply with mandatory minimum requirements. The inability of states to demand high-performance electronic voting machines due to the patchwork requirements of various state election laws would no longer be an issue and every state and county would be assured of the best machine the industry could create.

CONCLUSION

The current members of the investigative agency of Congress, the Government Accountability Office, have acknowledged that problems with electronic voting security do exist. Those same members have also washed their hands of the matter. The only recourse the American people have against such blatant disregard of the risks associated with electronic voting is to inform their senators and representatives in Congress that they are con-

---

324. *See* Griffin, *supra* note 285, at 528.
325. 42 U.S.C. § 15371 (Supp. II 2002); *see also* U.S. ELECTION ASSISTANCE COMM'N, *supra* note 303, at 27-28.
326. Sabrina Eaton, *Groups Want Changes to Overcome Election Setbacks*, PLAIN DEALER, Dec. 8, 2004, at A11.
327. 320 F.3d 440 (3d Cir. 2003).
328. *Id.* at 444, 451.

cerned about these risks and vote them out of office if they fail to pass legislation correcting these problems. But will their votes be correctly recorded?

Stephanie Philips