University of Chicago Legal Forum

Volume 1995 | Issue 1 Article 21

Public Access to Vote-Counting Software

William A. Wright
William.Wright@chicagounbound.edu

Public Access to Vote-Counting Software

William A. Wright†

Most states explicitly authorize election districts to employ computer vote-counting systems.[1] Computerized vote counts are faster and more reliable than counting paper ballots by hand.[2] Consequently, computers counted over half of the votes cast in 1992.[3] When election officials apply computer technology to vote

---

† B.A. 1983, Purdue University; M.A. 1985, University of North Carolina; Ph.D. 1988, University of North Carolina; J.D. Candidate 1996, University of Chicago.

[1] See Ariz Rev Stat Ann § 16-441 (West 1984 & Supp 1994); Ark Code Ann § 7-5-604 (1993); Cal Elections Code § 19205 (West 1989 & Supp 1995); Colo Rev Stat Ann § 1-5-601 (West 1989 & Supp 1994); 15 Del Code Ann § 5000A (1993 & Supp 1994); Fla Stat Ann § 101.5604 (West 1982 & Supp 1994); Hawaii Rev Stat § 16-1 (1985 & Supp 1992); Idaho Code § 34-2402 (1981 & Supp 1994); 10 Ill Comp Stat § 5/24A-3 (West 1993); Ind Code Ann § 3-11-7.5-4 (West 1988 & Supp 1994); Iowa Code Ann § 52.2 (West 1991 & Supp 1994); Kan Stat Ann § 25-4403 (1986 & Supp 1992); Ky Rev Ann Stat §§ 117.377 *et seq* (1993 & Supp 1994); La Rev Stat Ann § 18:1391 (West 1979 & Supp 1995)(authorizing for counting absentee votes only); 21-A Me Rev Stat Ann § 809 (1993 & Supp 1994); Md Election Code Ann §§ 16A-1 *et seq* (1993 & Supp 1994)(authorizing for specific counties only); Mass Ann Laws ch 54, §§ 32 *et seq* (Michie/Law Co-op 1990 & Supp 1995); Mich Comp Laws Ann § 168.794a (West 1989 & Supp 1994); Minn Stat Ann § 206.82 (West 1992 & Supp 1995); Miss Code Ann § 23-15-463 (1990 & Supp 1994); Mo Ann Stat § 115.229 (Vernon 1980 & Supp 1995); Neb Rev Stat §§ 32-4,113 *et seq* (1984 & Supp 1992); Nev Rev Stat § 293B.105 (1991); NH Rev Stat Ann § 656:40 (Equity 1986 & Supp 1994); NJ Stat Ann § 19:53A-2 (West 1989 & Supp 1994); NM Stat Ann §§ 1-9-17 *et seq* (1991 & Supp 1994); NC Gen Stat § 163-161 (1991 & Supp 1994); ND Cent Code § 16.1-06-11 (1991 & Supp 1993); Ohio Rev Code Ann §§ 3506.02 *et seq* (Banks 1994 & Supp 1995); 26 Okla Stat Ann § 3-104 (West 1991 & Supp 1995); Or Rev Stat § 246.530 (1993); 25 Pa Stat Ann § 3031.2 (Purdon 1994); RI Gen Laws § 17-19-3.4 (1990 & Supp 1994); SC Code Ann § 7-13-1310 (Law Co-op 1977 & Supp 1994); SD Cod Laws § 12-17B-3 (1982 & Supp 1994); Tenn Code Ann § 2-9-110 (1985 & Supp 1994); 17 Vt Stat Ann § 2491 (Equity 1982 & Supp 1994); Va Code §§ 24.2-626 *et seq* (1993 & Supp 1994); Wash Rev Code Ann § 29.33.020 (West 1993 & Supp 1995); W Va Code § 3-4A-1 (1994 & Supp 1994); Wis Stat Ann § 5.76 (West 1986 & Supp 1994); Wyo Stat § 22-11-102 (1992 & Supp 1994). See also Ala Code § 17-9-2 (1988 & Supp 1994)(not explicitly authorizing computerized voting systems); Ga Code Ann §§ 21-2-351, 21-2-365 (Michie 1993 & Supp 1994)(same); NY Election Law §§ 7-200 *et seq* (McKinney 1978 & Supp 1995)(same). Other states do not explicitly authorize computerized voting systems, but do have security plans for them. See Conn Gen Stat Ann § 9-238 (West 1989 & Supp 1994); Tex Election Code Ann §§ 51.031, 121.001 *et seq* (Vernon 1986 & Supp 1995); Utah Code Ann § 20-18-1 (1991 & Supp 1994).

[2] Gary Stix, *The Ø's Have It; Can Digital Ballot Boxes Keep Elections Honest?*, Sci Am 24 (Nov 1990).

[3] Id. See also National Clearinghouse of Election Administration, *A Report to the Congress on the Development of Voluntary Engineering and Procedural Performance Standards for Voting Systems* § 2.1 at 10 (U.S. Government Printing Office, 1984)("NCEA

counting, however, they create new problems. If contractors, computer programmers, and other experts control the process of tallying votes, how can the public assure themselves that the vote count will be fair and accurate?[4]

Current state law imposes some security safeguards on vote-counting computers and software.[5] The Federal Election Commission ("FEC") has suggested additional safety measures for future state enactment ("FEC Guidelines").[6] In part I, this Comment discusses both current and suggested security provisions, and argues that they do not adequately assure the public an accurate and fair vote count because they allow only elected officials, partisan representatives, and employees of those representatives to inspect the software. Public access to vote-counting software, in addition to the current security measures, would better guarantee a fair and unmanipulated vote count. In part II, this Comment argues that vote-counting software should be available for public inspection under many states' Freedom of Information laws. Unfortunately, the FEC suggests that states act to prevent Freedom of Information access to vote-counting software.[7] Contrary to the FEC position, this Comment suggests in part III that public access to vote-counting software is consistent with a public policy of protecting the commercial interests of software vendors.

I. STATE LAW AND FEC GUIDELINES PROVIDE LIMITED SECURITY FOR VOTE-COUNTING SOFTWARE

Some attempts to automate vote-counting systems ended in equipment failures.[8] Other problems resulted from management

---

Report")(estimating use of computerized vote-counting systems—including ballot scan, punch card, and purely electronic devices—as 66 percent of the population).

[4] In its recommendation that the Federal Election Commission ("FEC") develop voluntary standards for voting systems, the FEC National Clearinghouse Advisory Panel concluded that the "ultimate purpose of voluntary standards is to assist state and local officials in assuring the public of the integrity of our election system." NCEA *Report* § 2.3 at 23 (cited in note 3).

[5] See notes 14-47 and accompanying text.

[6] See United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (U.S. Government Printing Office, 1990)("FEC *Standards*").

[7] United States Federal Election Commission, *System Escrow Plan for the Voting System Standards Program* § 9.0 at 12 (U.S. Government Printing Office, 1990)("FEC *Escrow Plan*"), reprinted in FEC *Standards* (cited in note 6).

[8] In one case, a power surge "wiped out the vote counting program." A local college student had to write a new program to count the votes. National Clearinghouse of Election Administration, *A Report to the Congress on the Development of Voluntary Engineer-*

error.[9] Aside from accidental system errors and good faith mistakes, however, critics of computerized vote-counting systems have charged that unscrupulous operators could manipulate the programs during the vote count:[10]

> [A] certain pattern of holes in an otherwise innocuous looking vote card, one that looks to the outsider like all the others in a stack, might quietly reprogram the . . . machine and alter its final tabulations with nary a sign to election watchers. This change in logic might be triggered by accident, but, more disturbing to election specialists, it might also be initiated as part of an illegal scheme to fix a close election.[11]

All of the states that permit computerized vote-counting systems have enacted security provisions to insure that the software is free of errors and to prevent software tampering.[12] The

---

ing and Procedural Performance Standards for Voting Systems § 2.2 at 15-16 (U.S. Government Printing Office, 1984)("NCEA *Report*")(cited in note 3).

[9] For example, in 1984, in Carrol County, Maryland, an automated recount on an independently managed computer system showed a vote-counting error. In the original count, the system operator had inadvertently substituted a test version of the software for the final version. The required pre-election tests did not detect the substitution because the tests required the machine to read only one punch per column, while the actual election had a more complicated ballot. Roy G. Saltman, *Accuracy, Integrity, and Security in Computerized Vote-Tallying*, 31 Comm of the Assoc for Comp Mach 1184 (Oct 1988).

[10] John W. Verity, *Machine Politics*, Datamation 54, 54-55 (Nov 1, 1986). See also Saltman, 31 Comm of the Assoc for Comp Mach at 1187 (noting a lack of public confidence in operators of automated systems)(cited in note 9). For allegations of manipulation, see *Barrera v Superior Court*, 117 Ariz 528, 573 P2d 928 (Ariz App 1977)(recounting sought by unsuccessful candidate to investigate possible manipulation of vote counting system); *Palm v Lesher*, 489 SW2d 351, 352 (Tex Civ App 1973)(seeking recount using "independent and neutral operators and . . . corrected computer programs . . . ."); *Enterprise Residents Legal Action Against Annexation Committee v Brennan*, 22 Cal 3d 767, 587 P2d 658 (1978)(alleging that local election officials "made errors" and "an error in the vote-counting program or summation of ballot counts."); *Ryan v Bd of Election Commissioners of DuPage County*, 1994 US Dist LEXIS 13010, *2 (N D Ill)(alleging that "the computer software program used . . . to tally the votes fraudulently miscounted the votes").

[11] Verity, Datamation at 54-55 (cited in note 10).

[12] See Alaska Stat § 15.20.620 (1988 & Supp 1994); Ark Code Ann § 7-5-611 (1993); Ariz Rev Stat Ann §§ 16-445 *et seq* (West 1984 & Supp 1994); Cal Elections Code §§ 19103 *et seq* (West 1989 & Supp 1995); Colo Rev Stat Ann §§ 1-5-602 *et seq* (West 1989 & Supp 1994); Conn Gen Stat Ann § 9-242(c) (West 1989 & Supp 1994) (adopting FEC Guidelines); 15 Del Code Ann §§ 5001A *et seq* (1993 & Supp 1994); Fla Stat Ann §§ 101.5605 *et seq* (West 1982 & Supp 1994); Ga Code Ann § 21-2-359 (Michie 1993 & Supp 1994); Hawaii Rev Stat § 16-42 (1985 & Supp 1992); Idaho Code §§ 34-2410 *et seq* (1981 & Supp 1994); 10 Ill Comp Stat §§ 5/24A-8 *et seq* (West 1993 & Supp 1995); Ind Code Ann §§ 3-11-7-2, 3-11-7.5-26 (West 1988 & Supp 1994); Iowa Code Ann §§ 52.5 *et seq* (West 1991 & Supp 1994); Kan Stat Ann §§ 25-4406 *et seq* (1986 & Supp 1992); Ky Rev Ann Stat §§ 117.379 *et seq* (1993 & Supp 1994); La Rev Stat Ann § 18:1392 (West 1979 & Supp 1995)(-

FEC has provided additional voluntary guidelines designed to enhance security.[13] Unfortunately, both the current and suggested security measures fail to assure the public that election officials themselves cannot manipulate the vote-counting system.

A. Current and Suggested Security Provisions

Current state security provisions and the FEC suggested guidelines fall into several rough categories: technical requirements, pre-election tests, audit trails, and access security.[14] Because the Florida provisions[15] include some version of all these security measures, they serve as an excellent illustrative model.

1. *Technical requirements.*

Anyone who owns a vote-counting system and wants Florida to allow its use in the state must submit a copy of the software to the Florida Department of State ("Department").[16] At the owner's expense,[17] the Department employs a computer expert to test all software operations, including memory and logic components.[18]

---

for counting absentee ballots); 21-A Me Rev Stat Ann §§ 812 *et seq* (1993 & Supp 1994); Md Election Code Ann §§ 16A-1 *et seq* (1993 & Supp 1994)(for Montgomery County); Mass Ann Laws ch 54, §§ 33F *et seq* (Michie/Law Co-op 1990 & Supp 1995); Mich Comp Laws Ann §§ 168.795 *et seq* (West 1989 & Supp 1994); Minn Stat Ann § 206.83 (West 1992 & Supp 1995); Miss Code Ann §§ 23-15-465, 23-15-481, 23-15-507 (1990 & Supp 1994); Mo Ann Stat §§ 115.225 *et seq* (Vernon 1980 & Supp 1995); Neb Rev Stat §§ 32-4,116 and 32-4,120 (1984 & Supp 1992); Nev Rev Stat § 293B.063 (1991)(adopting the FEC Guidelines as of 1997); NH Rev Stat Ann §§ 656:41 *et seq* (Equity 1986 & Supp 1994); NJ Stat Ann §§ 19:53A-3 *et seq* (West 1989 & Supp 1994); NM Stat Ann §§ 1-9-14 *et seq* (1991 & Supp 1994); NY Election Law §§ 7-206 *et seq* (McKinney 1978 & Supp 1995); NC Gen Stat § 163-160 (1991 & Supp 1994); ND Cent Code §§ 16.1-06-14 *et seq* (1991 & Supp 1993); Ohio Rev Code Ann §§ 3506.05 *et seq* (Banks 1994 & Supp 1995); 26 Okla Stat Ann § 7-107.1 (West 1991 & Supp 1994); Or Rev Stat §§ 246.550 *et seq* (1993); 25 Pa Stat Ann §§ 3031.5 *et seq* (Purdon 1994); RI Gen Laws § 17-19-3.5 (1990 & Supp 1994); SC Code Ann §§ 7-13-1330 *et seq* (Law Co-op 1977 & Supp 1994); SD Cod Laws §§ 12-17B-5 *et seq* (1982 & Supp 1994); Tenn Code Ann § 2-9-110 (1985 & Supp 1994); Tex Election Code Ann §§ 122.001 *et seq* (Vernon 1986 & Supp 1994); Utah Code Ann § 20A-4-104 (1991 & Supp 1994); 17 Vt Stat Ann § 2499 (Equity 1982 & Supp 1994); Va Code §§ 24.2-629 *et seq* (1993 & Supp 1994); Wash Rev Code Ann §§ 29.33.041 *et seq* (West 1993 & Supp 1995); W Va Code §§ 3-4A-8 *et seq* (1994 & Supp 1994); Wis Stat Ann §§ 5.84 *et seq* (West 1986 & Supp 1994); Wyo Stat §§ 22-11-103 *et seq* (1992 & Supp 1994).

[13] United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (U.S. Government Printing Office, 1990)("FEC *Standards*")(cited in note 6).

[14] Id.

[15] Fla Stat Ann §§ 101.5605 *et seq*.

[16] Fla Stat Ann § 101.5605(1) (West 1982 & Supp 1994).

[17] Fla Stat Ann § 101.5605(2)(b) (West 1982 & Supp 1994).

[18] Fla Stat Ann § 101.5605(2)(a) (West 1982 & Supp 1994). The FEC Guidelines also

The FEC Guidelines' technical requirements go beyond testing memory and logic components. Software must be written in small sections with readily identifiable functions.[19] Each such module must be testable independently of the remainder of the program, and the program must not be self-modifying.[20] In addition, the FEC prefers that the crucial elements of the program use a "high level programming language,"[21] such as Pascal, COBOL, FORTRAN, or C. The modular structure of these languages makes programming errors easier to detect.[22]

2. *Pre-election tests.*

Once election officials acquire a vote-counting system, they must test it before each election.[23] Representatives of the political parties, the press, and the public may attend such tests.[24] Each political party may designate a computer expert to observe the test and the final vote.[25] To test the system, the operators punch a set of sample ballot cards[26] and use the vote-counting system to total these test cards.[27] Then the operators check the results against the predetermined totals to verify that the system can both record votes for each candidate and proposition and reject invalid ballots.[28] The operators run the same test immediately before and after the actual vote count.[29]

---

require an acceptance test performed by the jurisdiction acquiring the vote counting system to verify that the system, as delivered and installed, functions as required. FEC *Standards* § 8.1 at 91 (cited in note 6).

[19] FEC *Standards* § 4.2 at 45 (cited in note 6). Other suggestions include specific control constructs (for example, sequence, if-then-else, or do-while constructs), intelligible naming conventions, consistent coding conventions, uniform comments, and the absence of extraneous code. FEC *Standards*, Appendix E.

[20] FEC *Standards* § 4.2 at 45 (cited in note 6).

[21] Id at 46.

[22] Id.

[23] Fla Stat Ann § 101.5612(1) (West 1982 & Supp 1994). See also FEC, *Standards* §§ 2.1.1.5 and 2.2.1.6 at 9-10 (cited in note 6).

[24] Fla Stat Ann § 101.5612(1).

[25] Id.

[26] Fla Stat Ann § 101.5612(2) (West 1982 & Supp 1994).

[27] Id.

[28] Id. For example, in primary elections, the system might reject Democratic ballots marked for Republican candidates, or in general elections the system might have to reject ballots marked for more than one candidate for an office. See Fla Stat Ann § 101.5606(5) (West 1982 & Supp 1994).

[29] Fla Stat Ann § 101.5612(2). See also Alaska Stat §§ 15.20.620(d), (f) (1988 & Supp 1994) (requiring a manual count of six random precincts during the automated count, and allowing party representatives or state officials to request a listing of software code during the automated count). In the absence of tests in the middle of the vote count, the possibility that programmers will alter the vote-counting system while it is counting re-

3. *Audit trails.*

Vote-counting software must produce records adequate for a postelection audit of the election results.[30] The FEC Guidelines include exhaustive requirements for such an "audit trail."[31] A time and date stamp must appear on every record.[32] Records created before the vote count must identify the polling place and the software that produced them,[33] and the records must include the results of the diagnostic tests performed on the system components.[34] The audit trail must also include the ballot format,[35] sample ballots,[36] the total number of ballots cast,[37] vote totals for each contest,[38] and the number of ballots read within each precinct.[39] Finally, the records must include, in language that is easy to understand, all computer messages that occur during operation, and a statement of the operator response to each message.[40]

4. *Access security.*

Finally, the FEC Guidelines require that software include "measures to prevent access by unauthorized persons, and to prevent unauthorized operations by any person."[41] These measures include software protections, such as passwords, as well as hardware protections, such as devices to prevent people from connecting other machines to the vote-counting computer.[42] To reduce the risk of interference with the vote-counting system from

---

mains open. The programmer could change the program back at the end of the vote count.

[30] Fla Stat Ann § 101.5606(12) (West 1982 & Supp 1994). According to the FEC Guidelines, the audit trail increases public confidence in the accuracy of the tally, provides for recounts, and serves as evidence in litigation. FEC *Standards* § 4.8 at 49 (cited in note 6).

[31] FEC *Standards* § 4.8.1.1 at 50-51 (cited in note 6).

[32] Id at 50.

[33] FEC *Standards* § 4.8.2.2 at 52 (cited in note 6).

[34] Id.

[35] FEC *Standards* § 4.8.2.1 at 52 (cited in note 6).

[36] Id.

[37] FEC *Standards* § 4.8.2.4 at 54 (cited in note 6).

[38] Id. Contests include elections between candidates and elections for specific legislative measures.

[39] Id.

[40] FEC *Standards* §§ 4.8.1.2, 4.8.2.3 at 51, 53-54 (cited in note 6).

[41] FEC *Standards* § 5.3 at 56 (cited in note 6).

[42] FEC *Standards* § 5.3.2 at 57 (cited in note 6). Also, election officials may not permanently install software on a machine unless they store the machine in a secure location and have secure procedures for handling, preparing, and transporting it. FEC *Standards* § 5.5 at 58-59 (cited in note 6).

other programs, the FEC also suggests that operators run vote-counting software on a computer dedicated solely to that purpose and not on machines that run other programs simultaneously.[43]

Florida law requires vendors to submit a final copy of the software and all its documentation to the Department.[44] The FEC Guidelines instead suggest an escrow program that calls for the deposit of software, documentation, and other materials with a third party who is neutral between the vendor and election authority.[45] If something damages the working copy of the software, or if there is suspicion of fraud, election officials can use the copy on deposit to replace the damaged program, or to detect unauthorized alterations.[46] Furthermore, election officials have access to the software and documentation even if the vendor's business fails.[47]

B. Current and Suggested Security Provisions Are Inadequate

A state that adopts the FEC Guidelines would have a comprehensive set of security provisions for vote-counting software.[48] Even such a comprehensive set of safeguards would be inadequate, however, to assure the public of a vote count that is accurate and fair. It would be inadequate because the choice of an expert to test the software, the acquisition of the software, and the performance of the pre-election software tests remain in the hands of elected officials.[49]

Under current state law and the FEC Guidelines, state authorities are responsible for hiring an expert to examine the logic and code of vote-counting software.[50] However, state officials have a personal interest in the outcome of elections, and vendors of election software have a financial interest in securing contracts

---

[43] FEC *Standards* § 5.6.1 at 59-60 (cited in note 6).

[44] Fla Stat Ann § 101.5607(1)(a) (West 1982 & Supp 1994).

[45] United States Federal Election Commission, *System Escrow Plan for the Voting Systems Standards Program* § 2.0 at 1-2 (U.S. Government Printing Office, 1990)("FEC *Escrow Plan*")(cited in note 7), reprinted in FEC *Standards* (cited in note 6).

[46] Id.

[47] FEC *Escrow Plan* § 3.0 at 2 (cited in note 47).

[48] Compare Nev Rev Stat § 293B.063 and Conn Gen Stat Ann § 9-242(c) (adopting the FEC Guidelines) with 26 Okla Stat Ann § 7-107.1 (requiring only that voting machines register zero votes before count).

[49] See notes 14-29 and accompanying text.

[50] The FEC Guidelines include suggestions for the accreditation of independent testing authorities, but without Congressional funding the selection of the testing authority remains in the hands of state officials. United States Federal Election Commission, *A Process for Evaluating Independent Test Authorities* (U.S. Government Printing Office, 1990), reprinted in FEC *Standards* (cited in note 6).

for their products.[51] The public might reasonably fear that unscrupulous vendors would provide software that consistently gave elections to the reigning party, and that corrupt state officials would select an expert who would accept the flawed code without protest.

Recount provisions in state election laws may be an inadequate check on such conspiracies, because citizens who petition for a recount face imposing barriers. Some states only allow candidates to petition for a recount in certain elections.[52] Some states impose fees or security deposits on petitioners.[53] Petitioners might also have to offer proof of fraud or error before a court will grant the request for a recount.[54]

The FEC's proposed escrow plan[55] is also inadequate to detect a conspiracy between state election officials and vendors. Under the FEC Guidelines, once the state's expert certifies the software, a neutral escrow company keeps the master copy.[56] Local election officials use this escrow copy to detect tampering by comparing the working copy with the master.[57] However, this

---

[51] Gary Stix, *The Ø's Have It; Can Digital Ballot Boxes Keep Elections Honest?*, Sci Am 24 (Nov 1990)(cited in note 2).

[52] See, for example, 10 Ill Comp Stat § 5/23-1.2a (West 1993 & Supp 1995)(requiring that for statewide elections, petitioner must be a candidate, a write-in candidate, or submit at least as many signatures as would be required to become a candidate); Ind Code Ann § 3-12-6-2 (West 1988 & Supp 1994)(only candidates may petition); 25 Pa Stat Ann § 3313 (Purdon 1994)(requiring a petition with 100 signatures to contest elections for Governor or Lieutenant Governor); Tex Election Code Ann § 212.022 (Vernon 1986 & Supp 1995)(requiring a close election, counting errors in one or more precincts, or low total vote count). But see Cal Elections Code § 17160 (West 1989 & Supp 1995)(allowing any voter to contest an election); 10 Ill Comp Stat § 5/23-19 (West 1993 & Supp 1995)(allowing voters to contest any election except for elections for statewide offices).

[53] See, for example, Cal Elections Code § 17163 (West 1989 & Supp 1995)(requiring the requester to pay costs of the recount, unless requester's candidate receives a plurality of the votes cast); 10 Ill Comp Stat § 5/23-23 (West 1993 & Supp 1995)(requiring a deposit as security for court-determined costs); 25 Pa Stat Ann § 3459 (Purdon 1994)(requiring bond to pay all costs in case petitioner is found liable). But see Ind Code Ann § 3-12-6-10 (West 1988 & Supp 1994)(requiring only a deposit of $100 to recount up to ten precincts and $10 for each additional precinct).

[54] See DC Code Ann § 1-1315 (1992 & Supp 1994)(granting recount only for defects "serious enough to vitiate the election as a fair expression of the will of the . . . electors"); Fla Stat Ann § 102.168 (West 1982 & Supp 1994)(requiring the petitioner to "set forth the grounds on which [petitioner] intends to establish his right to such office or [to] set aside" the result); 10 Ill Comp Stat § 5/23-23.2 (West 1993 & Supp 1995)(requiring reasonable likelihood the recount will change the results); 25 Pa Stat Ann § 3457 (Purdon 1994)(requiring petitioners to present an affidavit that "according to the best of their knowledge and belief" the election was illegal and the return incorrect in order to contest elections for certain offices).

[55] See notes 45-47 and accompanying text.

[56] FEC *Escrow Plan* § 3.0 at 1 (cited in note 7).

[57] Id at 2.

arrangement will not detect a conspiracy between state officials and vendors because the flawed code is in the original software. Comparing the two copies will show no discrepancies.

Under these circumstances, the public must depend on the pre-election test to detect a conspiracy between state officials and vendors.[58] If the pre-election test was typically a thorough test of all the capabilities of the software, the public could safely rely on it. Unfortunately, it is not.[59]

Since election officials must pre-audit the deck of ballot cards used to test the vote-counting system, there is a practical limit on the number of cards in the deck. One plaintiff who sought access to vote-counting software under state Freedom of Information laws[60] explained how such a limited test might fail to detect vote-count manipulation.[61] The program could redirect votes from one party or candidate to another only after reaching some high threshold.[62] So, for example, if there were 250,000 voters in the county, and the pre-election test used only 35,000 ballot cards, then the program could redirect votes after correctly counting 35,000 ballots. Consequently, even if state law permits the public to be present at the pre-election test of vote-counting software, the test may not allay fears of fraud in the vote count.

In theory, election officials could increase public confidence in the vote-counting software in several ways, but most are dissatisfying. The officials could conduct public tests on a scale guaranteed to uncover any possible programmed manipulation of the count. Conceivably, the test could verify that the program would report every possible combination of ballots. However, the need to pre-audit the test cards and the possible permutations of vote results makes such a thorough test unlikely. States could authorize increased access to the vote-counting system for candidates, but candidates, especially for low prestige offices, may not pursue their rights vigorously. If they do not, then nothing would protect the public's interest in having a demonstrably fair vote count.[63] The Federal Government could certify the software, but

---

[58] Id (invoking the need for testing and access security).

[59] See notes 60-62 and accompanying text.

[60] *Ryan v DuPage County Bd. of Election Commissioners*, No. 2-92-1393 (Ill App, December 21, 1994)(appeal filed)(reading Illinois statute as exempting all software from disclosure). The appellate court affirmed the decision not to grant access, citing a specific provision of the Illinois Freedom of Information Act, 5 Ill Comp Stat 140/7¶ (West 1993 & Supp 1995).

[61] *Ryan*, No. 2-92-1393, slip op at 2.

[62] Brief for Plaintiff, *Ryan v DuPage County Bd. of Election Commissioners*, No. 92-CH-957 (Ill Cir Ct, Du Page County, 1994), aff'd by *Ryan*, No. 2-92-1393.

[63] As evidence that the public interest is separable from the candidates, see note 53

this would only shift public fears of manipulation to the national level. Finally, election officials could abandon computerized systems and return to counting votes by hand, but the delay in obtaining an accurate count has made this option unpopular.[64]

Perhaps the only practical means to assure the public that computer vote tallies are fair and accurate is to allow interested members of the public to obtain a copy of vote-counting software or to inspect the software and documentation. Citizens could then submit the material to their own expert for an evaluation of the program logic and possible security breaches.[65] This remedy would be available under state Freedom of Information laws.[66]

II. STATE FREEDOM OF INFORMATION LAWS WOULD GRANT PUBLIC ACCESS

All fifty states have adopted Freedom of Information or Open Government laws.[67] Many of these acts follow the general struc-

---

concerning state provisions for citizens to petition for a recount.

[64] Stix, Sci Am at 24 (cited in note 2).

[65] See the description of the tests performed by state-appointed experts at notes 18-29 and accompanying text.

[66] See notes 67-110 and accompanying text.

[67] Ala Code § 36-12-40 (1991 & Supp 1994); Alaska Stat §§ 09.25.110 *et seq* (1994); Ariz Rev Stat Ann §§ 39-121 *et seq* (West 1985 & Supp 1994); Ark Code Ann §§ 25-19-101 *et seq* (1992 & Supp 1993); Cal Govt Code §§ 6250 *et seq* (West 1980 & Supp 1995); Colo Rev Stat Ann §§ 24-72-201 *et seq* (West 1990 & Supp 1994); Conn Gen Stat Ann §§ 1-15 *et seq* (West 1988 & Supp 1994); 29 Del Code Ann §§ 10001 *et seq* (1991 & Supp 1994); DC Code Ann § 1-1521 (1992 & Supp 1994); Fla Stat Ann §§ 119.01 *et seq* (West 1982 & Supp 1995); Ga Code Ann §§ 50-18-70 *et seq* (Michie 1994); Hawaii Rev Stat §§ 92F-1 *et seq* (1985 & Supp 1992); Idaho Code §§ 9-337 *et seq* (1990 & Supp 1994); 5 Ill Comp Stat §§ 140/1 *et seq* (West 1993 & Supp 1995); Ind Code Ann §§ 5-14-3-1 *et seq* (West 1989 & Supp 1994); Iowa Code Ann §§ 22.1 *et seq* (West 1989 & Supp 1994); Kan Stat Ann §§ 45-215 *et seq* (1986 & Supp 1992); Ky Rev Ann Stat §§ 61.870 *et seq* (1993 & Supp 1994); La Rev Stat Ann §§ 44:31 *et seq* (West 1982 & Supp 1995); 1 Me Rev Stat Ann §§ 401 *et seq* (1989 & Supp 1994); Md State Govt Code Ann § 10-613 (1993 & Supp 1994); Mass Ann Laws ch 66, § 10 (Michie/Law Co-op 1991 & Supp 1995); Mich Comp Laws Ann §§ 15.231 *et seq* (West 1994); Minn Stat Ann §§ 13.03 *et seq* (West 1988 & Supp 1995); Miss Code Ann §§ 25-61-1 *et seq* (1991 & Supp 1994); Mo Ann Stat §§ 109.180 *et seq* (Vernon 1966 & Supp 1995); Mont Code Ann §§ 2-6-102 *et seq* (1993); Neb Rev Stat §§ 84-712 *et seq* (1987 & Supp 1993); Nev Rev Stat §§ 239.010 *et seq* (1991); NH Rev Stat Ann §§ 91-A:1 *et seq* (Equity 1990 & Supp 1994); NJ Stat Ann §§ 47:1A-1 *et seq* (West 1989 & Supp 1994); NM Stat Ann §§ 14-2-1 *et seq* (1988 & Supp 1994); NY Public Officers Law §§ 84 *et seq* (McKinney 1988 & Supp 1995); NC Gen Stat §§ 132-1 *et seq* (1993 & Supp 1994); ND Cent Code § 44-04-18 (1993); Ohio Rev Code Ann §§ 149.43 *et seq* (Banks 1994 & Supp 1995); 51 Okla Stat Ann §§ 24A.1 *et seq* (West 1988 & Supp 1995); Or Rev Stat §§ 192.410 *et seq* (1993); 65 Pa Stat Ann §§ 66.1 *et seq* (Purdon 1959 & Supp 1994); RI Gen Laws §§ 38-2-1 *et seq* (1990 & Supp 1994); SC Code Ann §§ 30-4-10 *et seq* (Law Co-op 1991 & Supp 1994); SD Cod Laws §§ 1-27-1 *et seq* (1992 & Supp 1994); Tenn Code Ann §§ 10-7-503 *et seq* (1992 & Supp 1994); Tex Govt Code Ann §§ 552.001 *et seq* (Vernon 1994); Utah Code

ture of the Federal Freedom of Information Act ("Federal Act").[68] The Federal Act creates a presumption that, upon request, federal agencies must disclose any record in their possession to any member of the public.[69] To forestall public disclosure, the agency must invoke one of seven specific exemptions.[70] In any state that follows the Federal Act, the public should be able to obtain vote-counting software, if (1) the state classifies software as disclosable records, (2) a government agency holds the software, and (3) no exemption prevents disclosure.

A. Vote-Counting Software Is a Disclosable Record in an Agency's Possession

A few states' Freedom of Information laws differ from the Federal Act by explicitly excluding computer software from the class of disclosable records.[71] Election officials in these states currently have no duty to disclose vote-counting software under Freedom of Information laws. Other states, especially those that

---

Ann §§ 63-2-101 *et seq* (1993 & Supp 1994); 1 Vt Stat Ann §§ 315 *et seq* (Equity 1985 & Supp 1994); Va Code §§ 2.1-340 *et seq* (1987 & Supp 1994); Wash Rev Code Ann §§ 42.17.270 *et seq* (West 1991 & Supp 1995); W Va Code §§ 29B-1-1 *et seq* (1993 & Supp 1994); Wis Stat Ann §§ 19.31 *et seq* (West 1986 & Supp 1994); Wyo Stat §§ 16-4-201 *et seq* (1990 & Supp 1994).

[68] 5 USC §§ 552 *et seq* (1994)("Federal Act"). When a person requests a record from a federal agency, the agency has ten days to respond. 5 USC § 552(a)(6)(A)(i). If the agency denies the request, citing one of the seven exemptions, then the requester may appeal the decision to the head of the agency. 5 USC § 552(a)(6)(A). If the head of the agency also refuses to disclose the record, the requester may file suit in district court. 5 USC § 552(a)(4)(B). The court will examine the issue *de novo* and, if it finds for the plaintiff, may require the agency to disclose the record. Id. Furthermore, if the plaintiff "substantially prevails," the court may award attorney fees. 5 USC § 552(a)(4)(E). Connecticut and Hawaii deviate from the Federal Act by creating public commissions to oversee government compliance. Connecticut gives the commission authority to hear appeals from administrative decisions. Conn Gen Stat Ann § 1-21j (West 1988 & Supp 1994). Hawaii makes appeal to the commission an alternative to judicial review. Hawaii Rev Stat § 92F-15.5 (1985 & Supp 1992).

[69] 5 USC § 552(a)(3).

[70] 5 USC § 552(b).

[71] See Cal Govt Code § 6254.9(a) (West 1980 & Supp 1995) (exempting software developed by government agency from public record); Colo Rev Stat Ann § 24-72-202(7) (West 1990 & Supp 1994)("'writings' . . . does not include computer software."); Utah Code Ann § 63-2-103(18)(b)(iv) (1993 & Supp 1994)(exempting proprietary software). See also RI Gen Laws § 38-2-2(d)(2) (1990 & Supp 1994)(exempting trade secrets from public records); 1 Vt Stat Ann § 317(b)(9) (Equity 1985 & Supp 1994)(exempting trade secrets from records). See also Wis Stat Ann § 19.32(2) (West 1986 & Supp 1994)(exempting copyrighted materials).

rely on interpretations of the Federal Act in construing their own Freedom of Information laws,[72] should classify vote-counting software as a disclosable record.

One district court found that software may be a disclosable record under the Federal Act.[73] In *Cleary, Gottlieb, Steen & Hamilton v Department of Health and Human Services*,[74] the plaintiffs sought access to a computer program written by a government consultant. The government argued that a computer program is not a record under the Federal Act;[75] a "record" preserves information, while a program is "merely a list of instructions for a computer to manipulate a database."[76] Nevertheless, the court concluded that computer programs could be disclosable records under the Federal Act for two reasons. First, the Supreme Court had found that records include "'machine readable materials . . . regardless of physical form or characteristics.'"[77] Second, the program requested in *Cleary* was "uniquely suited" to the database.[78] Consequently, the program's design reflected the author's understanding of what data in the database was significant and what was not.[79] The program thus preserved information and was a disclosable record.[80]

---

[72] See *State Bd. of Equalization v Superior Court*, 10 Cal App 4th 1177, 13 Cal Rptr 2d 342 (1992); *Bd. of Trustees of Woodstock Academy v Freedom of Information Comm'n.*, 181 Conn 544, 436 A2d 266 (1980); *Faulk v State's Attorney for Harford County*, 299 Md 493, 474 A2d 880 (1984); *State Employees Ass'n. v Dept. of Management and Budget*, 428 Mich 104, 404 NW2d 606 (1987); *Fink v Lefkowitz*, 47 NY2d 567, 393 NE2d 463 (1979); *Michael v Communications Workers of America*, 130 Misc 2d 424, 495 NYS2d 569 (1985); *Quirk v Evans*, 116 Misc 2d 554, 455 NYS2d 918 (1982); *Burke v Yudelson*, 81 Misc 2d 870, 368 NYS2d 779 (1975), aff'd by 51 AD2d 673, 378 NYS2d 165 (1976); *Texas Dept. of Public Safety v Gilbreath*, 842 SW2d 408 (Tex App 1992); *Dawson v Daly*, 120 Wash 2d 782, 845 P2d 995 (1993); *Hearst Corp. v Hoppe*, 90 Wash 2d 123, 580 P2d 246 (1978). But see *Newark Morning Ledger Co. v Saginaw County Sheriff*, 204 Mich App 215, 514 NW2d 213 (1994)(holding that differences from the Federal Act reduce the value of federal interpretations); *McReady v Dept. Consumer & Regulatory Affairs*, 618 A2d 609 (DC App 1992)(requiring a likelihood that legislative body was aware of judicial interpretation of the Federal Act).

[73] *Cleary, Gottlieb, Steen & Hamilton v HHS*, 844 F Supp 770, 782 (D DC 1993)(holding that programs that are "uniquely suited" to a database preserve information and perpetuate knowledge and thus are agency records under the Federal Act, but exempting the particular software as "predecisional" and "deliberative").

[74] 844 F Supp 770.

[75] Id at 781.

[76] Id.

[77] Id at 782, quoting *Forsham v Harris*, 445 US 169, 183 (1980).

[78] *Cleary, Gottlieb, Steen & Hamilton*, 844 F Supp at 782.

[79] Id at 782-83.

[80] Id. The district court ultimately found that one of the specific exemptions in the Federal Act covered the requested program, but the ruling that a computer program can be a public record still stands.

These same two reasons apply to vote-counting software. The software is machine-readable material, which the Federal Act does not exclude from the class of records. Moreover, vote-counting software contains specific information regarding the relative weight accorded each vote cast. In all cases where the program counts the votes fairly, the information contained in the program will be the trivial information that for each vote cast for a candidate the candidate receives one tally. In a case where the computer does manipulate the vote count, the program will contain the shocking information that some votes—possibly those counted after the first 35,000—do not receive the usual weight. If the program diverts the votes to another candidate, the votes will have a negative relative value for the voter's candidate. These weights are crucial information recorded in the software—no less so if all the programs in use weight the votes properly.

States that rely on interpretations of the Federal Act should also find that a government agency holds the vote-counting software. In *United States Department of Justice v Tax Analysts*,[81] the Supreme Court ruled that for material to be disclosable a government agency "must 'create or obtain'"[82] the material, and the material must "come into the agency's possession in the legitimate conduct of its official duties."[83] Local election officials might not create vote-counting software themselves, but they obtain the software for use in the elections they administer.[84] Therefore, the software arguably comes into their possession in the legitimate conduct of their duties. Consequently, election officials in many states should disclose the software, unless they can specify an exemption that prevents disclosure.[85]

---

[81] 492 US 136 (1989)(holding that a record created or obtained by an agency meets a prerequisite for being disclosable under the Federal Act).

[82] Id at 144, quoting *Forsham*, 445 US at 182.

[83] *Tax Analysts*, 492 US at 145.

[84] See note 1.

[85] See notes 69-70 and accompanying text.

B. Exemptions May Not Apply

Some states have enacted specific exemptions for software.[86] One state provides for confidentiality of vote-counting software in the state election code,[87] but many others follow the Federal Act and have no exemptions directly applicable to vote-counting software. In order to block public access to the software under Freedom of Information laws, officials in these states would probably have to rely on the state acts' exemptions for trade secrets.[88]

The trade secret exemption is one of the seven exemptions in the Federal Act. "[T]rade secrets and commercial or financial information obtained from a person and privileged or confidential . . ." are exempt from public disclosure.[89] This trade secret exemption has analogues in many state acts.[90]

---

[86] See Fla Stat Ann § 119.07(3)(q) (West 1982 & Supp 1995)(exempting software that is licensed to a public body and a is trade secret); Ga Code Ann § 50-18-72(f)(2) (Michie 1994)(exempting programs used or maintained by a public body in the course of operations); Idaho Code § 9-340(16) (1990 & Supp 1994)(exempting software); 5 Ill Comp Stat § 140/7¶ (West 1993 & Supp 1995)(exempting software where disclosure would endanger the security of the data processing system); Ind Code Ann § 5-14-3-4(b)(11) (West 1989 & Supp 1994)(exempting software entrusted to a public body); Kan Stat Ann § 45-221(a)(16) (1986 & Supp 1992)(exempting software); Mo Ann Stat § 610.021(10) (Vernon 1988 & Supp 1995)(exempting software codes for data processing); ND Cent Code § 44-04-18.4(2)(a) (1993)(exempting software subject to a copyright); 51 Okla Stat Ann § 24A-10(B)(3) (West 1988 & Supp 1995)(exempting software if disclosure would give an unfair advantage to competitors); Or Rev Stat § 192.501(16) (1993)(exempting software purchased for the public body's own use); Va Code § 2.1-342(B)(16) (1987 & Supp 1994)(exempting vendor proprietary software).

[87] See Tex Govt Code Ann § 552.101 (Vernon 1994)(exempting "information considered to be confidential by law"); Tex Election Code Ann § 122.0331 (Vernon 1986 & Supp 1995)(declaring electronic voting system codes on file with the Secretary of State not to be public information).

[88] The FEC suggests enactment of a trade secret exemption to protect vote counting software from public disclosure. United States Federal Election Commission, *System Escrow Plan for the Voting Systems Standards Program* § 9.0 at 12-13 (U.S. Government Printing Office, 1990)("FEC *Escrow Plan*")(cited in note 7), reprinted in United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (U.S. Government Printing Office, 1990)("FEC *Standards*")(cited in note 6).

[89] 5 USC § 552(b)(4) (1988).

[90] See Ark Code Ann § 25-19-105(9)(A) (1992 & Supp 1993)(exempting "[f]iles which, if disclosed, would give advantage to competitors or bidders"); Colo Rev Stat § 24-72-204(3)(a)(IV) (West 1990 & Supp 1994)(exempting "[t]rade secrets, privileged information, and confidential commercial, financial, geological, or geophysical data furnished by or obtained from any person"); Conn Gen Stat Ann § 1-19(b)(5) (West 1988 & Supp 1994)(exempting trade secrets defined to include "commercial or financial information given in confidence, not required by statute"); 29 Del Code Ann § 10002(d)(2) (1991 & Supp 1994)(exempting "[t]rade secrets and commercial or financial information obtained from a person which is of a privileged or confidential nature"); DC Code § 1-1524(a)(1) (1992 & Supp 1994)(exempting "[t]rade secrets and commercial or financial information

If a state's Freedom of Information law relies only on the trade secret exemption to protect vote-counting software, the software is still likely to be disclosable. Judicial interpretations of the Federal Act's trade secret exemption hold records to be exempt if they are: (1) information that is (a) commercial or financial, (b) obtained from a person, and (c) privileged or confidential; or (2) trade secrets.[91] Given the significance of the public interest in a demonstrably fair election, vote-counting software is neither commercial or financial information, nor a trade secret under the Federal Act.

1. *Commercial or financial information.*

Vote-counting software is not exempt from disclosure under the first prong of the trade secret exemption. In federal cases

---

obtained from outside the government, to the extent that disclosure would result in substantial harm to the competitive position of the person from whom the information was obtained"); Ga Code Ann § 50-18-72(b)(1) (Michie 1994)(exempting "[a]ny trade secrets obtained from a person or business entity which are of a privileged or confidential nature and required by law to be submitted to a government agency . . ."); Hawaii Rev Stat § 92F-13(3) (1985 & Supp 1992)(exempting records that must be confidential to avoid frustrating a legitimate government interest); Iowa Code § 22.7(3) (West 1989 & Supp. 1994)(exempting trade secrets protected by law); Md State Govt Code Ann § 10-617(d) (1993 & Supp 1994)(exempting trade secrets and confidential commercial or financial information); Mich Comp Laws Ann § 15.243(13)(1)(g) (West 1994)(exempting trade secrets or commercial information provided to a public body under an authorized promise of confidentiality); Minn Stat Ann § 13.37(2) (West 1988 & Supp 1995)(exempting trade secrets); Miss Code Ann § 25-61-9(3) (1991 & Supp 1994)(exempting trade secrets and confidential commercial or financial information); Mont Code Ann § 2-6-110(1) (1993)(applying confidentiality and business secrets to computer records); Neb Rev Stat § 84-712.05(3) (1987 & Supp 1993)(exempting trade secrets and other proprietary or commercial information which would give advantage to business competitors and serve no public interest); NH Rev Stat Ann § 91-A:5(IV) (Equity 1990 & Supp 1994)(exempting confidential commercial or financial information); NY Public Officers Law § 87(2)(d) (McKinney 1988 & Supp 1995)(exempting trade secrets or information from a commercial enterprise which would cause substantial injury to the competitive position of the enterprise); NC Gen Stat § 132-1.2 (1993 & Supp 1994)(exempting trade secrets, private property, and confidential information); SC Code Ann § 30-4-40(a)(1) (Law Co-op 1991 & Supp 1994)(exempting trade secrets as unpatented, secret plans and processes used in preparing trade commodities); Tex Govt Code Ann § 552.110 (Vernon 1994)(paralleling the Federal Act); W Va Code § 29B-1-4(1) (1993 & Supp 1994)(exempting trade secrets as unpatented, secret plans or processes having commercial value and giving a competitive advantage); Wyo Stat § 16-4-203(d)(v) (1990 & Supp 1994)(exempting trade secrets, privileged information, and confidential commercial or financial information obtained from any person). See also *State ex rel. Jacobs v Prudoff*, 30 Ohio App 3d 89, 506 NE2d 927 (1986)(holding that trade secrets defined in Ohio Rev Code Ann § 1333.51(c) are exempt from disclosure under Ohio Rev Code Ann § 149.43(A)(1)).

[91] See *Getman v NLRB*, 450 F2d 670, 673 (DC Cir 1971). But see *Barceloneta Shoe Corp. v Compton*, 271 F Supp 591 (D Puerto Rico 1967)(holding that the trade secret provision exempts: (1) trade secrets; (2) commercial or financial information; and (3) privileged or confidential information).

interpreting this provision, "commercial" and "financial" receive their ordinary meanings.[92] Examples of these categories include audits and financial statements,[93] memoranda analyzing salary proposals,[94] test results necessary for receiving marketing approval for a product,[95] intrastate sales information,[96] and cost justifications for service rates.[97] Against this background, vote-counting software does not constitute commercial or financial information.

2. *Trade secrets.*

Vote-counting software is probably not exempt under the trade secret exemption either. In *Public Citizen Health Research Group v Food and Drug Administration*,[98] the court defined "trade secret" for the Federal Act's exemption as a "secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort."[99] The court rejected the Restatement of Torts definition of a trade secret as "any formula, pattern, device, or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[100] The

---

[92] See *Public Citizen Health Research Group v Food and Drug Administration*, 704 F2d 1280, 1290 (DC Cir 1983); *Allnet Communication Services, Inc. v FCC*, 800 F Supp 984, 988 (D DC 1992).

[93] See *National Parks and Conservation Ass'n. v Morton*, 498 F2d 765, 770 (DC Cir 1974).

[94] See *9 to 5 Org. for Women Office Workers v Bd. of Governors of Federal Reserve System*, 721 F2d 1, 3 (1st Cir 1983).

[95] *Public Citizen*, 704 F2d at 1290.

[96] See *Continental Oil Co. v Federal Power Comm'n.*, 519 F2d 31, 35 (5th Cir 1975), overruled on other grounds as *Superior Oil Co. v Federal Energy Regulation Comm'n.*, 563 F2d 191 (5th Cir 1977); *Sharyland Water Supply Corp. v Block*, 755 F2d 397, 398 (5th Cir 1985).

[97] *Allnet Communication*, 800 F Supp at 988.

[98] 704 F2d at 1288.

[99] Id.

[100] 4 Rest Torts § 757 comment (b) (1939), cited in *Public Citizen*, 704 F2d at 1286. Four states appear to have incorporated elements of the Restatement's definition into their Freedom of Information laws: Ark Code Ann § 25-19-105(9)(A) (exempting files which would give advantage to competitors); Neb Rev Stat § 84-712.05(3) (exempting trade secrets and other proprietary or commercial information which would give advantage to business competitors and serve no public interest); NY Public Officers Law § 87(2)(d) (exempting trade secrets or information from a commercial enterprise which would cause substantial injury to the competitive position of the enterprise); W Va Code § 29B-1-4(1) (exempting trade secrets as unpatented, secret plans or processes having commercial value and giving a competitive advantage). See also 51 Okla Stat Ann § 24A-

court's preferred definition focuses on whether the owner of a secret uses it to produce goods,[101] not on whether the owner would suffer competitive harm from disclosure of the secret.[102]

No owner of a trade secret has successfully prevented disclosure under *Public Citizen*'s definition.[103] Nevertheless, vendors of vote-counting software might plausibly argue that disclosure of their software would reveal secret programming techniques used to produce the software. Assuming that the programming techniques incorporated into vote-counting software are "commercially valuable . . . process[es] . . . used for the making . . . of trade commodities,"[104] courts would likely balance the "innovation or substantial effort"[105] behind the techniques against the public interest in disclosure.

Courts interpret exemptions to the Federal Act narrowly, to maximize public access to government records.[106] In light of that policy, courts are likely to read the requirement of innovation or effort as reducing the number of secret processes that government agencies would otherwise disclose. To determine the precise restrictions on the trade secret exemption, courts are likely to appeal to the legislative purposes of the Federal Act.[107] Engaging in such an analysis, the courts would weigh the impor-

---

10(B)(3) (exempting software if disclosure would give an unfair advantage to competitors). Others appear simply to follow the *Public Citizen* definition. See Conn Gen Stat Ann § 1-19(b)(5) (exempting trade secrets defined as "unpatented, secret, commercially valuable plans, appliances, formulas, or processes, which are used for the making, preparing, compounding, treating or processing of articles or materials which are trade commodities obtained from a person and which are recognized by law as confidential, and commercial or financial information given in confidence, not required by statute"); SC Code Ann § 30-4-40(a)(1) (exempting trade secrets as unpatented, secret plans and processes used in preparing trade commodities). To the extent that a state's exemptions require a showing of competitive harm, the court's balancing of interests will parallel the policy argument in notes 111-137 and accompanying text.

[101] *Public Citizen*, 704 F2d at 1290.

[102] Id at 1288. One reason for this interpretation is that the Restatement definition of "trade secrets" would have rendered the fourth exemption's "commercial and financial information" prong moot. Competitive harm is central to the courts' analysis of the latter clause.

[103] But see *Anderson v Department of Health and Human Services*, 907 F2d 936, 944 (10th Cir 1990)(remanding defendant's application of the trade secret exemption for reconsideration in light of the *Public Citizen* definition, but stating in dicta that "'manufacturing and processing information, including formulations, chemistry and quality assurance procedures' are probably within the narrow definition . . . .").

[104] *Public Citizen*, 704 F2d at 1288.

[105] Id.

[106] *Tax Analysts*, 492 US at 151.

[107] See *National Parks*, 498 F2d at 767 (looking to legislative purposes to give meaning to "confidential" in the trade secret exemption).

tance of disclosure to "'the functioning of a democratic society'"[108] against the government interest in efficient operation,[109] individual interests in privacy,[110] and the vendors' property interests. Because they have rejected the Restatement's definition of trade secrets, the courts will not have to balance any competitive injury the vendor might suffer from disclosure. Since public confidence in vote-counting procedures is critical to the functioning of a democracy, no privacy interests are at stake, and the government faces little expense in making vote-counting software available to the public, courts performing this analysis are unlikely to prevent disclosure.

Since vote-counting programs are disclosable records in the possession of a government agency, the Federal Act would require that the agency disclose it to members of the public on request. No specific exemption in the Federal Act would block this disclosure, and the trade secret exemption probably would not apply. In these circumstances, any state that relies on interpretations of the Federal Act should also have a legal duty to disclose vote-counting software. The FEC recognized this possibility in its Guidelines and argues against public disclosure.

III. THE FEC ARGUES AGAINST PUBLIC ACCESS

Nevertheless, the FEC has suggested that state and local government bodies should not disclose vote-counting software to the public.[111] The FEC specifically identified an escrow company's immunity from Freedom of Information requests as an advantage of the Guidelines' escrow plan over other alternative arrangements.[112] The FEC also suggested that states without an escrow plan should amend their Freedom of Information laws

---

[108] *Tax Analysts*, 492 US at 142, quoting *National Labor Relations Board v Robbins Tire & Rubber Co.*, 437 US 214, 242 (1978).

[109] *National Parks*, 498 F2d at 767.

[110] Id.

[111] United States Federal Election Commission, *System Escrow Plan for the Voting Systems Standards Program* § 9.0 at 12 (U.S. Government Printing Office, 1990)("FEC *Escrow Plan*")(cited in note 7), reprinted in United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (US Government Printing Office, 1990)("FEC *Standards*")(cited in note 6).

[112] FEC *Escrow Plan* § 3.0 at 2 (cited in note 7). Since an independent escrow company is not a government agency, arguably, it would be immune from Freedom of Information claims.

to exempt trade secrets from public disclosure and that vendors should require their governmental clients to sign "confidentiality, non-disclosure agreements."[113]

Two concerns lie behind the FEC's suggestions. First, the FEC fears that public access to the software might endanger the "security and integrity of the electoral process."[114] Second, the FEC fears that vendors might suffer competitive harm.[115] If the public may obtain the software or documentation under Freedom of Information laws, so may the vendor's competitors.[116]

A. The FEC Suggestions Are Unnecessary

The FEC is too pessimistic in assuming that public access to vote-counting software would endanger the security of the system. If a member of the public obtains a copy of the software, and the original remains unchanged, there is no added danger of vote-count manipulation.[117] Even if election officials allow the public to test the original software on the original machine, the FEC Guidelines require the design of the software to prevent changing the program while in operation.[118] In addition, the usual security arrangements and the escrow copy of the software remain, allowing election officials to detect tampering.

The FEC, however, is too optimistic in thinking that escrow plans or trade secret exemptions to Freedom of Information laws will protect vote-counting software from public disclosure. To the extent that states rely on federal precedents in interpreting their own Freedom of Information laws,[119] the public should have access to the software that election officials actually use.[120] A master copy of the program on deposit with an escrow company should make no difference to the citizens' right. Similarly, reliance on trade secret exemptions should not prevent public access to vendor supplied software.[121]

---

[113] FEC *Escrow Plan* § 9.0 at 12-13 (cited in note 7).

[114] FEC *Escrow Plan* § 3.0 at 2-3 (cited in note 7). The FEC's fear for the integrity of the process seems to focus on local election authorities, but the same concern arises for public access.

[115] FEC *Escrow Plan* § 9.0 at 13 (cited in note 7).

[116] Id.

[117] See *Ryan v DuPage County Bd. of Election Commissioners*, No. 2-92-1393, slip op at 3 (Ill App, December 21, 1994)(appeal filed)(defendants' expert testified that to manipulate the vote count would require a conspiracy of all vendors and election officials).

[118] FEC *Standards* § 4.2 at 45 (cited in note 6).

[119] See note 71.

[120] See note 67-110 and accompanying text.

[121] See notes 86-110 and accompanying text.

Nevertheless, variations of the FEC suggestions would succeed in protecting software from public disclosure. If the state does not classify software as disclosable records, then vote-counting software will not be disclosable.[122] Similarly, if the state exempts all software—or vote-counting software specifically—from public disclosure, then election officials may withhold the vote-counting software.[123] A final justification of public disclosure for vote-counting software, therefore, requires a reason not to amend Freedom of Information laws to protect vote-counting software. The following sections argue that copyright law already protects the vendors' commercial interests to some extent, and that the social cost of blocking public access to the software outweighs the social benefit of any further protection.

B. Copyright Law Provides Some Protection For Vendors' Interests

Vendors might be eligible for copyright protection for their interests in vote-counting software. Copyright legally prevents anyone from making an unauthorized copy of the software.[124] This prohibition extends not only to the software code, but to any structural element of the program design that is not essential to accomplishing the program's purpose.[125] For example, copyright might protect the specific commands operators use to control the program and the image the program produces on the screen.[126] Copyright therefore protects the vendors' interest in the software by insuring that other software producers will not simply copy the program, or specific elements of it. Copyright does not offer complete protection, however, since courts have limited the protection software enjoys,[127] and since other producers might benefit from the vendors' software without copying it.

Courts have imposed three limits on copyright protection of software. First, copyright does not protect elements of a program that are the most efficient means of achieving the program's

---

[122] See note 71 and accompanying text.

[123] See notes 86-87 and accompanying text.

[124] 17 USC § 106 (1994).

[125] *Whelan Associates, Inc. v Jaslow Dental Laboratory, Inc.*, 797 F2d 1222, 1236 (3d Cir 1986).

[126] Kenneth W. Dam, *Some Economic Considerations in the Intellectual Property Protection of Software*, 24 J Legal Stud (manuscript at 26)(copy on file with the *University of Chicago Legal Forum*).

[127] See notes 128-130 and accompanying text.

purpose.[128] Second, copyright does not protect elements that are necessary due to technical requirements of the computer equipment or the industry the program serves.[129] Finally, copyright does not protect information taken from the public domain.[130]

These general limits on copyrights in software raise questions regarding protection specifically for vote-counting software. Software which meets the FEC guidelines is simple in structure and contains no excessively complicated code;[131] the vendors' software must be very efficient. Consequently, much of the code might not receive copyright protection. In addition, the facts of democratic elections dictate many elements of vote-counting software. For example, a simple input device such as a punch card or a panel of buttons is necessary because of the number of people who must use the system. Any element of the software necessary to meet such industry requirements might not receive copyright protection.

The limits on copyright protection for software increase the risk that other producers will benefit from legitimate access to vendors' programs. Copyright law permits other producers to examine software and to discover secret programming techniques in the software, so long as they do not make an unauthorized copy in the process. Consequently, even when vendors have a copyright, other producers may still obtain a legitimate copy of the program—through purchase or under Freedom of Information laws—and discover any secret programming techniques the vendors might have used. Other producers may discover the most efficient way of counting votes on a computer from the original vendors' program, and save themselves the expense of research and development. Therefore, the crucial issue for the debate over public access to vote-counting software is whether the vendors' interest in preventing such reverse engineering merits protection beyond copyright law.

---

[128] *Computer Associates Int'l, Inc. v Altai, Inc.*, 982 F2d 693, 707-08 (2d Cir 1992). See also Dam, 24 J Legal Stud (manuscript at 26)(cited in note 126).

[129] *Computer Associates*, 982 F2d at 709-10. See also Dam, 24 J Legal Stud (manuscript at 26)(cited in note 126).

[130] *Computer Associates*, 982 F2d at 710. See also Dam, 24 J Legal Stud (manuscript at 26)(cited in note 126).

[131] FEC *Standards* § 4.2 at 45, Appendix E (cited in note 6).

C. The Balance of Interests Favors Public Access

Protections for intellectual property impose social costs. One social cost is the lack of access to useful ideas. When other producers may not access innovative programming techniques, the public cannot benefit from the lower costs and improved services that market competition in the software would provide. Generally, the social benefits that copyright and other protections provide outweigh this social cost. By securing profits to the original vendor for a limited time, society encourages programmers and vendors to innovate and to create new technologies.[132]

Under the FEC Guidelines, vendors of vote-counting software would benefit from two protections of intellectual property: copyright and the denial of public access under Freedom of Information laws. As protections of intellectual property, the justification for these protections is to encourage software development.[133] However, for vote-counting software, the denial of public access would impose a second social cost: the lack of public confidence in the vote-counting system. If states permitted public access to vote-counting software, they would remove this second social cost, but vendors would still have significant market advantages over other producers.

Before other producers would have any incentive to mimic vendors' software, and before they would have access to the software through Freedom of Information laws, the original vendors must sell or lease vote-counting software to election officials. Vendors secure two benefits by being first in the particular market. First, local election officials invest time and effort in the software. They are likely to resist learning a new program.[134] While courts limit copyright protection, they are likely to prohibit other producers from marketing a program with the "look and feel" of the vendors' software.[135] Consequently, the election officials' investment of time in the vendors' software creates a barrier other producers must overcome to enter the market.[136]

---

[132] William M. Landes and Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J Legal Stud 325 (1989).

[133] Besides the intellectual property argument, a second justification for restricting public access is to prevent tampering or fraud. But see notes 114-118 and accompanying text.

[134] See Dam, 24 J Legal Stud (manuscript at 36-38)(cited in note 126).

[135] Id (manuscript at 26).

[136] Id (manuscript at 38-40).

Second, vendors can reinforce the election officials' vendor-specific investment by selling documentation and services.[137] The election officials will need manuals, instruction, and technical support. These secondary products represent added investments and thus increase election officials' resistance to competing programs. Vendors might also find a small market in selling nontechnical documentation to those members of the public who wish to fully understand the vote-counting system.

Vendors might argue that, where other producers have access to their software through Freedom of Information laws, the other producers can quickly develop competing software and then capture a similar market position in other states or other election precincts. Public access does create this risk to the vendors' interests. In these circumstances, vendors would be wise to focus on the market for secondary products, and compete, not just on the merits of their software, but on the merits of the technical support and training they offer.

Even under a policy of public access to vote-counting software, vendors have copyright protection and the advantages of being first in the market. The rewards of this privileged position are probably adequate to encourage further refinements in vote-counting software. Nevertheless, allowing public access would remove a protection available to the vendors under the FEC Guidelines. A significant social benefit is necessary to justify that sacrifice. In the case of vote-counting software, the significant social benefit is easy to identify: the public confidence that vote counts are fair and accurate.

CONCLUSION

Early stories of equipment failure and possible mismanagement produced public fears of manipulation of computerized vote-counting systems.[138] In response, the FEC suggested additional security measures for computerized vote-counting systems.[139] If administered by honest officials, these security measures should

---

[137] Id (manuscript at 19).

[138] National Clearinghouse of Election Administration, *A Report to Congress on the Development of Voluntary Engineering and Procedural Performance Standards for Voting Systems* § 2.2 at 12-16 (U.S. Government Printing Office, 1984)("NCEA *Report*")(cited in note 3).

[139] See generally FEC *Standards* (cited in note 6).

detect any errors or alterations in vote-counting systems. However, those security measures do not address the public fear of vote manipulation.[140]

The FEC specifically rejects a policy of public access to vote-counting software under state Freedom of Information laws.[141] Even though the policy would allow the public to verify that vote-counting software is correct and fair, the FEC argues that it endangers the vendors' commercial interests.[142]

Despite the FEC's intuitive misgivings, the principles of intellectual property justify enhanced public access to vote-counting software. Vendors have secured a strong position in the voting system market by being first in that market. They can exploit this position by selling secondary products such as documentation, training, and technical support. Meanwhile, election officials' investment of time in the software encourages vendor loyalty. These advantages should be sufficient to encourage software development. While maintaining this significant social benefit, states can also secure the benefit of increased public confidence in vote-counting software by providing for public access to that software.

---

[140] NCEA *Report* § 2.2 at 12 (cited in note 3).

[141] FEC *Escrow Plan* § 9.0 at 12-13.

[142] Id.