Vote Counting, Technology, and Unintended Consequences

Michael A. Carrier
VOTE COUNTING, TECHNOLOGY, AND UNINTENDED CONSEQUENCES

MICHAEL A. CARRIER†

TABLE OF CONTENTS

INTRODUCTION .............................................................................. 646

I. VOTING SYSTEMS, ERRORS, AND FRAUD .................................. 647
   A. Voting Systems ........................................................................... 647
   B. Errors .......................................................................................... 649
       1. Residual Votes ........................................................................... 650
       2. Other Errors ............................................................................. 650
   C. Fraud .......................................................................................... 653
       1. Non-DRE Technologies ............................................................ 653
       2. DREs ....................................................................................... 654
          a. Homebrew Smartcards ....................................................... 657
          b. Administrator Smartcards ............................................... 658
          c. Ballot Definition ............................................................... 659
          d. Vote Records .................................................................... 660
          e. Audit Logs ......................................................................... 662
          f. External Communications ................................................. 663
       3. Central Tabulators ................................................................. 663
   D. Partisan Affiliations ................................................................. 666

II. 2004 ELECTION ........................................................................ 668
   A. Inaccuracies ................................................................................. 668
   B. Circumstantial Evidence ............................................................ 672
       1. Exit Polls .................................................................................. 672
       2. Incumbent Performance in Pre-election Polls ..... 675
       3. Ohio: Phantom Votes, Undervotes, Unusual
          Turnouts, and Preordained Recounts ..................................... 677

III. RECOMMENDATIONS .................................................................. 680

Copyright © 2005 by Michael A. Carrier.
† Associate Professor, Rutgers University School of Law—Camden. I would like
   to thank Kevin Baker, Greg Lastowka, Harry Litman, Dennis Patterson, and David
   Silver for helpful comments on this Article, and Julie Assis, Gabriella Ferri, Melissa
   Fisher, and Dave Tseng for valuable research assistance.
CONCLUSION

INTRODUCTION

The 2000 presidential election had a searing effect on this nation. Few who witnessed the events in Florida could displace the images of election officials peering at punch cards, struggling to determine the intent of voters. Congress, for example, did not forget. Congress did not wish to see the scenes from Florida replayed in future elections. And so, in 2002, it enacted the Help America Vote Act, known as “HAVA,” which provided $325 million to the states to replace their punch card voting systems.¹

Many states have enthusiastically embraced this invitation, replacing punch cards with electronic voting machines, known as direct recording electronic devices (DREs). Given the rapidly approaching 2006 deadline to upgrade, other states are currently considering such activity.

In the rush to solve one problem, however, states may be creating another, far greater, one. To be sure, DREs relieve election officials of the challenge of ascertaining the voters’ intent. They also allow for expeditious counting, have the capability to reduce “undervotes” and “overvotes,” and promise to increase access for voters with disabilities. These benefits have been touted by election officials—Democrats and Republicans alike—who have adopted DREs.

But outside the computer science community, the full panoply of dangers from such systems has avoided scrutiny. This Article attempts to remedy this deficiency. In particular, it underscores several disturbing characteristics of electronic voting, including the following:

(1) Reduced transparency. Unlike boxes of paper ballots that materialize after the polls close, a hidden trap door in a software program counting millions of votes cannot be discovered.

(2) Increased magnitude of error and fraud. Because intangible computer software lacks the physical nature of paper ballots, it does not offer an upper limit on error and fraud.

(3) Lack of security controls. The refusal to use controls such as encryption makes it astonishingly easy to change vote totals, register votes for unintended candidates, prematurely terminate elections, and erase the "audit log" that is designed to trace such activity.

I supplement the analysis of the DRE software by examining vote counting flaws in the 2004 presidential election, including machine breakdowns, vote totals that exceeded or underrepresented the number of voters who cast ballots, and incidents in which the machines switched votes from one candidate to another (with ninety-eight of ninety-nine reported incidents involving switches favoring George Bush). I also collect circumstantial evidence such as exit polls that diverged from the official vote count to a greater extent than any other election in the modern era; an incumbent President's surpassing his standing in pre-election polls by a larger amount than in the past fifty years; and questionable voting patterns and activity in states such as Ohio. Although such evidence does not automatically prove the existence of error or fraud, it is more important than ever given the nontransparent nature of the vote counting process and inability to directly uncover fraud.

I conclude by offering recommendations to improve the accuracy and verifiability of vote counting today. In particular, I propose for electronic voting machines a voter-verified paper trail, random audits, open source software, more robust certification, and other recommendations. Only after these proposals are adopted can voters have confidence that the promise of vote counting technology will match its perils.

I. VOTING SYSTEMS, ERRORS, AND FRAUD

Five types of voting systems are used in the United States today. This section briefly introduces the systems and then explores the types of error and fraud associated with each. It concludes that the migration from paper ballots and punch cards to electronic voting, while offering the potential to reduce certain types of errors, also increases the potential magnitude of error and fraud and reduces the transparency of vote counting.

A. Voting Systems

Voters in U.S. elections today cast their vote on one of five types of voting equipment: paper ballots, mechanical lever
machines, punch cards, optical scan ballots, and DREs. The choice of voting technology is decentralized, with each of the nation’s more than 3,100 counties selecting the system it will use.

Paper ballots, the oldest technology, were the only system used during the first one hundred years of the nation. By the 2004 presidential election, however, they were used by only 0.6% of the electorate, in approximately three hundred rural counties. Voters using this system place a mark next to the name of their preferred candidate on a piece of paper, with the ballots later counted by hand.

Mechanical lever machines were developed in the 1890s. Although these machines are no longer manufactured, they are still employed in several states, with 12.8% of voters using them in the 2004 election. Voters using the machines enter a voting booth, close a curtain, flip small levers next to the names of the preferred candidates, and then pull a large lever that records the vote.

Punch card systems were first employed in 1964 and were used by 18.6% of the electorate in the 2004 election. In using this technology, voters employ a stylus to punch out small pieces of paper—the “chads” of 2000 election fame—from cards with small pre-scored perforations.

Optical scan systems, which are utilized for standardized


3 See Fischer, supra note 2, at 1; see also Brady et al., supra note 2, at 10 (noting that in the majority of states, voting systems are chosen by each county).

4 Fischer, supra note 2, at 2.


6 Fischer, supra note 2, at 3.


8 Fischer, supra note 2, at 3.

tests, were first employed for voting in the 1980s\textsuperscript{10} and were used by 32.2\% of the voters in the 2004 election. Voters using the technology fill in bubbles on a paper ballot with a pencil or other writing device. The ballot is then scanned—either within each precinct or at certain central locations—by a machine that senses and records the marks.\textsuperscript{11}

DRE machines were first introduced in the 1970s\textsuperscript{12} and were used by 28.9\% of voters in the 2004 election. The older generation of DREs, known as push-button systems, is similar to lever machines, but employs buttons that record votes electronically instead of levers. The newer technology, touch screen systems, allows voters to touch a computer screen to register their selection.\textsuperscript{13}

Of the five technologies used today, paper ballots, lever machines, and punch cards have declined in significance. This development can be explained in part by Congress's enactment of the Help America Vote Act of 2002, better known as HAVA.\textsuperscript{14} This statute provided $325 million to states that replaced their punch-card and lever voting machines by 2006.\textsuperscript{15} Only DREs and some optical scanners fully satisfy the requirements enunciated for voting systems.\textsuperscript{16}

B. Errors

The five systems described in the previous section differ in their error rates. This section describes numerous types of errors, including “residual votes” and other mishaps reported in recent elections.

\textsuperscript{10} FISCHER, supra note 2, at 3.
\textsuperscript{12} FISCHER, supra note 2, at 3.
\textsuperscript{13} BRADY ET AL., supra note 2, at 13; Election Assistance Commission, Direct Recording Electronic (DRE), http://www.eac.gov/election_resources/dre.htm (last visited July 23, 2005).
\textsuperscript{15} Id. § 102 (providing that states must commit to replacing their systems by the November 2004 election, extendible for good cause to the first general election held after January 1, 2006).
\textsuperscript{16} Id. § 301 (setting forth requirements such as voter verification and ability to correct ballots and access for individuals with disabilities).
1. Residual Votes

The category of residual votes includes uncounted ballots (cast by voters but not counted by election officials), undervotes (in which a voter does not select a candidate for an office), and overvotes (in which a voter selects too many candidates). Some of the undervotes, especially in races below the presidential race, are intentional, as the voter does not intend to vote for a candidate. But many others—including, according to one study, one and a half million votes in a typical presidential election—are unintentional.

The relative performance of the voting technologies has proven to be consistent in recent years. Nearly all studies have concluded that punch cards have performed the worst and precinct-count optical scans and touch-screen DREs have performed the best in the rates of residual votes.

A crucial determinant of the rate of residual votes is the ability to provide feedback to the voter at the time of voting. Precinct-based optical scans offer this opportunity because the ballot is fed into a scanner in front of the voter and rejected if it cannot be read, which allows the voter to remedy any deficiencies. Similarly, DREs and lever machines can be programmed to prevent overvotes. In contrast, paper ballots, punch cards, and centrally-scanned optical scan machines do not offer this opportunity for feedback to the voter.

2. Other Errors

In addition to residual votes, many other types of errors have plagued the vote counting process. Although these errors are

---

18 Id. at 21.
19 See David C. Kimball, Assessing Voting Methods in 2002, at 28 tbl. 2 (July 2004), available at http://www.umsl.edu/~kimball/dkmipsa2.pdf (finding residual vote rates in the 2002 gubernatorial elections of 3.5% and 2.8% for two types of punch cards, 1.3% for precinct-based optical scans, and 1.2% for touch screen DREs); see also BRADY ET AL., supra note 2, at 29 (finding that punch cards had the highest, and optical scans the lowest, residual vote rates in the 2000 presidential election).
often not as capable of precise delineation as residual votes, they
are equally important. This section provides an overview of the
types of errors associated with each of the voting technologies.

Paper ballots are subject to error because of the significant
human element involved in counting ballots. In contrast to the
other technologies, humans play a more important role in
counting, which introduces the possibilities of inattention and
fatigue.22 On the other hand, each of the other four types of
voting systems is subject to mechanical and other problems not
faced by paper ballots.

Lever machines have “an immense number of moving parts
that are subject to wear.”23 In particular, each time a voter pulls
down a lever, a counter wheel within the machine is turned one-
tenth of a full rotation.24 Error can result from excessive friction
in the connections. The higher frequency of vote totals ending in
“99”—as compared, for example, to “98” and “00”—suggests that
this may have in fact occurred in elections.25

The potential range of errors with punch cards was on full
display in the 2000 presidential election in Florida. Punch cards
jammed in readers, chads accidentally fell out, and pre-scored
punch cards were not fully removed when pushed with a stylus.26
As the 2000 election also revealed, it is difficult to determine the
voter’s intent when one or two of the chad’s corners are hanging
or when the hole is not completely punched through but is only a
“dimples chad.”27

Optical scan machines rely on the accuracy of the ballot
reader, which typically uses light or other media as a sensor
detecting the mark. The reader must be sensitive enough to read
the marks without mistaking smudges for votes. It also must
ensure that only one ballot is read at a time. For those ballots
counted at a central location, the delivery to the location
introduces opportunities for error, such as a mixup of ballots
from different precincts. And for precinct-counted ballots, the

22 ROY G. SALTMAN, ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED
VOTE-TALLYING § 3.2.1 (1988), available at http://www.itl.nist.gov/lab/specpubs/500-
158.htm.
23 Douglas W. Jones, A Brief Illustrated History of Voting § 5 (2003),
24 SALTMAN, supra note 22, § 3.3.
25 See id. § 3.3.2; see also Jones, supra note 23, § 5.
26 SALTMAN, supra note 22, §§ 3.4.1, 3.4.4.
27 Jones, supra note 23, § 6.
transmission of results over phone lines could lead to inaccuracies.\textsuperscript{28}

In recent years, the largest number of errors has accompanied the use of DREs. In the 2004 elections, for example, even though less than 30% of voters used the machines, at least 60% of reported election incidents concerned DREs.\textsuperscript{29} The errors affected machines by all of the major vendors, including Diebold, Hart Intercivic, Danaher, Election Systems and Software (ES&S), and Sequoia, although it especially plagued the latter three.\textsuperscript{30}

In large part, this is due to the important role played by, and questionable performance and security of, software in the machines. Software is notoriously subject to defects causing programs to malfunction. It is difficult to pinpoint each of the software flaws in DREs because the vendors treat the material as proprietary trade secrets. The likelihood of errors is increased by hardware defects and lax testing standards.\textsuperscript{31}

One example of a range of software flaws surfaced when Diebold left a version of its source code, or list of instructions causing the computer to operate, on an unprotected Internet site.\textsuperscript{32} Computer scientists obtained access to the code and were astonished at how poorly it was designed, with one commenting: "They made mistakes I wouldn't expect an undergraduate in computer security to make."\textsuperscript{33} Numerous flaws increase the likelihood of not only error but also fraud.

\textsuperscript{28} SALTMAN, supra note 22, §§ 3.5, 3.5.1, 3.6.1.
\textsuperscript{29} Deirdre Mulligan & Joseph Lorenzo Hall, Preliminary Analysis of E-Voting Problems Highlights Need for Heightened Standards and Testing, available at http://www7.nationalacademies.org/cstb/project_evoting.html (follow “Papers Received” hyperlink; then follow “Preliminary Analysis of E-Voting” hyperlink) (last visited July 23, 2005).
\textsuperscript{30} Id.
\textsuperscript{31} These concepts are further developed below. See infra notes 51–60 and accompanying text.
C. Fraud

Each of the five voting technologies used in the United States today is susceptible to fraud. The types of fraud, however, differ in their transparency, ease of execution, and potential magnitude. Along these axes, DREs pose the greatest danger.

1. Non-DRE Technologies

Stories of fraud in the use of paper ballots have appeared for centuries. Before the introduction in the late nineteenth century of the "Australian ballot" system—which limits the distribution of ballots to the polls where voters mark them in secret—ballots could be transported and candidates often bribed voters for their vote.34

Today, there are several ways to compromise paper ballots. One method is to make additional marks on the ballots for particular candidates, which subjects those ballots to invalidation in certain jurisdictions.35 Another is through a vote-counting process in which standards are interpreted by tally teams "well trained in the selective exclusion of votes for the opposition."36 A third type is the well-known "stuffing of the ballot box," with incidents that famously include:

- The 1948 Democratic Senate primary, in which Lyndon Johnson trailed his opponent by 854 votes when the polls closed but gained victory when additional ballots appeared, including 202 votes cast in alphabetical order.37
- The 1960 presidential race, in which John Kennedy won narrowly amid allegations of ballot stuffing, multiple voting, and voting by dead people in Illinois.38
- A 1997 referendum on the construction of a football stadium for the San Francisco Forty-Niners, in which more than one hundred ballot boxes—with an abundance of votes in favor of the proposition—appeared after the polls had closed, with the delay "attributed to 'wet ballots' that needed to be 'dried in a microwave oven.'"39

34 HARRIS, supra note 32, at 33; SALTMAN, supra note 22, § 3.2.
35 SALTMAN, supra note 22, § 3.2.1.
36 Jones, supra note 23, § 4.
37 HARRIS, supra note 32, at 35.
39 Election Fraud in the 1997 49er Stadium Election: 14 Points of Concern, ¶ 10
These potential instances of fraud may have altered the outcome in each of the cases. But they are transparent since the materialization of ballot boxes could be discovered. Moreover, the physical nature of the ballots limits the number of ballots that could be added. Nonetheless, the examples highlight the potential fraud associated with paper ballots.

Lever machines also are susceptible to several types of fraud. Party workers could cast extra votes on the machines, and technicians could tamper with the mechanical register behind each lever or insert incorrect identifying strips on the front of the machine. Of significant concern, lever machines lack an audit trail, which would make it difficult to trace any of these actions. On the other hand, fraud on lever machines tends to be localized, as each machine would need to be separately rigged.

Punch cards are subject to tampering by pre-punching the card for the desired candidate, which would invalidate as an “overvote” any selections of other candidates. Another possibility is to manufacture the cards so that the desired candidate’s chad is easier to punch out or the undesired candidate’s is harder to dislodge. Each of these methods of fraud is at least partly detectible given the physical nature of the cards.

Like punch cards, optical scan ballots may contain additional marks on the ballot for the favored candidate. Fraud can occur when ballots are counted at the precinct level (because the read-only memory is subject to tampering) or at a central location (where the transmission over phone lines and the central tabulation are subject to manipulation). As discussed below, the greatest concern with optical scanners is presented by the central tabulators that count all of the votes cast on machines throughout various counties.

2. DREs

The completely paperless nature of DREs, along with the role of computers in each stage of the vote counting process, ensures that, of the five types of voting technologies, DRE fraud

is least likely to be detected and most likely to have vast effects.\textsuperscript{45} In addition, DRE fraud is possible at each stage of the voting process: before the election (through physically unsecured machines), during voting (through smartcards that allow voters to gain unauthorized access), and after votes have been cast (through votes that are misrecorded when registered or tabulated).

A leading computer scientist explained that no one knows how “to find all the errors in a computer system; . . . to make sure that a system is secure or that it hasn't been corrupted; . . . and . . . to ensure that the systems in use are running the software they are supposed to be running.”\textsuperscript{46} These problems have not been solved even when technologists use “measures that are far more sophisticated (and costly) than those used in the design and certification of voting equipment.”\textsuperscript{47}

Nor is the examination of computer software any more transparent. Software is critical to DREs, with the success of elections “hing[ing] on the correctness, robustness, and security of the software.”\textsuperscript{48} But flaws in software are not easily detectable, as malicious computer code may be disguised as useful code or may be difficult to locate.\textsuperscript{49} These dangers are heightened in programs as complex as those used by DREs and in software that the voting machine vendors have jealously guarded as proprietary trade secrets.\textsuperscript{50}

\textsuperscript{45} One commentator has explained that paperless DREs appear to reduce fraud and error only by eliminating the ability to detect them and has analogized the situation to “trying to solve your accounting problems by eliminating your accounting department.” Kim Alexander, The Need for Transparent, Accountable and Verifiable U.S. Elections, YUBANET, ¶ 1, Dec. 11, 2004, http://www.yubanet.com/cgi-bin/artman/exec/view.cgi/10/16133.


\textsuperscript{47} Id.

\textsuperscript{48} KOHNO ET AL., supra note 32, at 3. My discussion of “software” in the text refers to a collection of programs, commonly referred to as Election Management Software (EMS), with functions that include controlling the ballot definition, prompting user-interface transactions (voting), maintaining recordkeeping, providing database security, and processing data.


\textsuperscript{50} Id. at 13 (noting that DRE software is complex because it “serves as a voter interface, records the ballot choices, and tallies the votes cast”); Editorial, Gambling on Voting, N.Y. TIMES, June 13, 2004, § 4, at 12.
For all of these reasons, the testing and certification process is critical. Nonetheless, this process is flawed. For starters, there is a “stunning lack of transparency” surrounding testing and certification, which the companies complete in secret and refuse even to discuss. And for another, the “independent” testing laboratories are chosen and paid by the vendors, with the consequence that they are “under enormous pressure to do reviews quickly, and not to find problems.” As the president of one of the companies conceded, “[t]here’s going to be the risk of a conflict of interest when you are being paid by the vendor that you are qualifying [the] product for.”

Even this lax certification is avoided when vendors install uncertified software, often immediately before elections. Such software was used, for example, by ES&S in three counties in Indiana and by Diebold in each of the seventeen counties in California in which it operated voting machines. A more well-known example occurred in Georgia in 2002. Shortly before the election, Diebold installed multiple versions of uncertified software in each of the state’s 22,000 voting machines allegedly to prevent the machines from freezing up. This activity gained added significance given the array of electoral surprises in the election.

Another software vulnerability results from voting machines’ lax physical security. Machines have been left for days at polling stations with pre-loaded ballots accessible to poll supervisors hired without background checks while other machines have

---

52 Id. For further doubt on the role played by certification, see infra Parts I.C.2.a–f (detailing numerous flaws with certified software).
53 Id.
54 Ian Hoffman, Electronic-Voting Critics Get Unusual Support From Labor, OAKLAND TRIB. (Cal.), Jan. 15, 2004; Mary Beth Schneider, Election Panel OKs Illegal Software, INDIANAPOLIS STAR, Mar. 11, 2004, at B2; see also HARRIS, supra note 32, at 189–90 (providing examples of counties in Arizona, California, Kansas, Texas, and Washington).
55 HARRIS, supra note 32, at 90–94.
56 See id. at 88 (discussing 2002 electoral surprises in Georgia and also noting a discovery on the Internet of a Diebold folder called “rob-georgia”). The upsets included that of triple-amputee Vietnam veteran Senator Max Cleland (who was leading in the pre-election polls but lost 53%–46%) and that of Governor Roy Barnes (who was leading by 9 to 11 points but lost 51%–46%). Posting by Unregistered User to http://www.votewatch.us/forums/general/497536620634 (Nov. 11, 2002, 1:27 PM).
been secured by only a bicycle lock with a combination known by poll supervisors and used at "every polling station in the county." As a result, anyone with access to the machines could alter software that controls, for example, the ballot definition or the termination of the election.

Even when the software is certified and the machines are secured, a disturbing number of vulnerabilities have been unearthed. Though not receiving much popular attention, computer scientists have consistently and emphatically stressed the ease with which fraud could occur. In some cases, the vendors themselves have conceded the potential for fraud. The remainder of this section details several vulnerabilities of DRE software and provides examples from recent elections that are consistent with these flaws. The discussion demonstrates that, of all the voting technologies used today, DREs are subject to the most far-reaching but least visible types of fraud.

a. Homebrew Smartcards

One way in which fraud could occur is through the use of "homebrew smartcards." When voters show up at the polling

---

58 Id.
60 DIEBOLD ELECTION SYSTEMS, CHECKS AND BALANCES IN ELECTIONS EQUIPMENT AND PROCEDURES PREVENT ALLEGED FRAUD SCENARIOS 12 (2003), available at http://www2.diebold.com/checksandbalances.pdf (conceding that "an election insider" would be able to attack the "data stored internally on each voting terminal"); see also infra notes 63 and 85 (detailing other Diebold concessions).
61 A smartcard is "a card, usually about the size of a credit card, with an
site, they are given smart cards that they insert into the DRE and that allows them to receive a ballot.\textsuperscript{62} Computer scientists found that attackers could create their own homebrew smartcards, which could be obtained from vendors selling programmable cards and which could be developed by “attach[ing] a ‘wiretap’ device between the voting terminal and a legitimate smartcard and observ[ing] the communicated messages.”\textsuperscript{63}

This danger was highlighted by the Compuware Report, a 246-page report commissioned by the state of Ohio, that examined the DREs of the four major vendors: Diebold, ES&S, Hart, and Sequoia. The report found that the four-digit PIN code for the smart card “is a factory default from Diebold [that] cannot be changed . . . [and] was guessed in less than two minutes of testing.”\textsuperscript{64} Voters who are able to program their own smartcards have the ability to vote multiple times on a machine by “ignor[ing] the voting terminal’s deactivation command.”\textsuperscript{65}

\textit{b. Administrator Smartcards}

Voters also could create their own “administrator cards,” which would allow them to act as supervisors and take actions such as terminating elections.\textsuperscript{66} One potential “safeguard” that Diebold could have employed to block this activity, a four-digit PIN code, turned out to be meaningless because every supervisor card used across the country has the same PIN: 1111.\textsuperscript{67} It is therefore not surprising that the Compuware Report concluded that “[t]here is a risk that an unauthorized person could learn the PIN number . . . and gain access to the supervisor functions on the machine,” which would include the ability to “close the polls early.”\textsuperscript{68}

Nor is the vulnerability of the supervisor functions limited to embedded computer chip that can communicate with another electronic device that can read information from and/or write it to the card.” \textsc{Fischer}, \textit{supra} note 49, at 14 n.48.

\textsuperscript{62} \textsc{Kohno et al.}, \textit{supra} note 32, at 7.

\textsuperscript{63} \textit{Id.} at 9. Diebold has conceded that “it would be possible to reverse engineer the password” that would allow the use of one’s own smartcard. \textsc{Diebold Election Systems}, \textit{supra} note 60, at 8.

\textsuperscript{64} \textsc{Compuware Report}, \textit{supra} note 59, at 52.

\textsuperscript{65} \textsc{Kohno et al.}, \textit{supra} note 32, at 10.

\textsuperscript{66} \textit{Id.} at 10–11.

\textsuperscript{67} \textsc{Compuware Report}, \textit{supra} note 59, at 57, 64, 72.

\textsuperscript{68} \textit{Id.}
Diebold. The supervisor password for the ES&S machines was not encrypted even though anyone with access to a supervisor card could vote multiple times, close an election early, or clear the machine of all votes cast.\(^69\) Similarly, a “zero-length password” on the Hart Intercivic machine could allow “an unauthorized person... [to] close the polls prematurely.”\(^70\) And even these systems seem secure in comparison to the Sequoia DRE, which allows any voter to terminate an election by flipping a button on the back of the machine.\(^71\)

These vulnerabilities are not merely hypothetical. Recent elections witnessed activity consistent with unauthorized access to administrator smartcards, including (1) the 2000 elections in Riverside County, California, in which a Sequoia DRE “unaccountably froze, then began counting backward;”\(^72\) (2) the 2002 elections in San Luis Obispo County, California, in which “a machine spontaneously began reporting totals with five hours left in the election;”\(^73\) and (3) the 2002 gubernatorial primary in Florida, in which many votes in Miami County “were not counted... because machines were shut down improperly,” with the consequence that one precinct “with over 1,000 eligible voters recorded no votes, despite a 33 percent turnout statewide.”\(^74\) To be clear, these events have not been proven to be a direct result of smartcard fraud. But they are in fact consistent with such fraud and they reveal the unique dangers of DREs.

c. Ballot Definition

Another type of fraud would alter the data stored internally in each DRE. One target could be the “ballot definition,” which provides details about the ballot such as precincts, races, and candidates.\(^75\) An attacker could change ballot definition files by programming the software to count votes for one candidate as votes for another candidate. Similarly, anyone working at a local Internet Service Provider (ISP) could tamper with the

\(^{69}\) Id. at 96; see also id. at 100 (noting that, of the three necessary passwords, “[t]wo... are hard-coded in the firmware and are only three characters in length”).

\(^{70}\) Id. at 156, 177.

\(^{71}\) Id. at 204–05.

\(^{72}\) O’Donnell, supra note 33.

\(^{73}\) Id.


\(^{75}\) COMPUWARE REPORT, supra note 59, at 12.
downloading of the ballot definition file from the Internet.\textsuperscript{76} Despite the danger of access to the ballot definition, none of the four major vendors have encrypted the data.\textsuperscript{77}

Errors consistent with altered ballot definition files have occurred in numerous elections, including (1) the 2000 presidential election in New Mexico, in which 67,000 votes were incorrectly counted because a worker used inaccurate party affiliations;\textsuperscript{78} (2) the 2002 election in Miami County, Florida, in which a change in the order of candidates in the ballot definition file resulted in an initial tally where the losing candidates appeared to win;\textsuperscript{79} (3) the September 2002 election in Union County, Florida, in which 2,642 Democratic and Republican votes were read as entirely Republican;\textsuperscript{80} and (4) the 2004 presidential election in Maryland, in which software “failed to record some votes correctly, jumped to other pages on the ballot without being prompted by the voter and inadvertently omitted some political races.”\textsuperscript{81} Occurrences such as these are typically called “glitches” or are blamed on human error.\textsuperscript{82} But whether due to error or fraud, they underscore the heightened scale of potential discrepancies resulting from the computerization of the vote counting process.

d. Vote Records

Another type of data fraud targets the records of all cast votes. Anyone with access to this data could alter vote records and “generate or change as many votes as he or she pleased.”\textsuperscript{83} Such votes “would be indistinguishable from the true votes cast

\textsuperscript{76} KOHNO ET AL., supra note 32, at 13–14.
\textsuperscript{77} COMPUWARE REPORT, supra note 59, at 36, 95, 170, 203.
\textsuperscript{78} KOHNO ET AL., supra note 32, at 13 n.3; Donna Young, Human Error is Cause of N.M. Election Glitch, GOVT COMPUTER NEWS, Nov. 20, 2000, available at http://www.gcn.com/vol19_no33/news/3307-1.html.
\textsuperscript{79} Oscar Corral, Technician’s Error, Not Machines, to Blame in Dade Election Mix-Up, MIAMI HERALD, Apr. 4, 2002, at 1A.
\textsuperscript{80} HARRIS, supra note 32, at 15.
\textsuperscript{82} See HARRIS, supra note 32, at 15 (discussing “programming errors”); Corral, supra note 79 (“A software technician made a mistake . . . and the . . . ballots were tallied based on the bad programming.”); Welsh, supra note 81 (blaming human error); Young, supra note 78 (“[A] county technical employee failed to set up an element of the system properly.”).
\textsuperscript{83} KOHNO ET AL., supra note 32, at 15–16.
on the terminal."\(^{84}\) But despite the critical importance of the vote records, one single Data Encryption Standard (DES) key, F2654hD4, has encrypted all of Diebold's vote records data since at least 1998.\(^{85}\) Not surprisingly, the testers in the Compuware study were easily able to "alter[] counts"\(^{86}\) on the Diebold DRE. The vote records also were vulnerable on other machines, as ES&S, Hart, and Sequoia each failed to encrypt the records.\(^{87}\) The Compuware testers were able to "read and manipulate" vote tallies on these systems as well.\(^{88}\)

Another danger, the multiple counting of votes, plagued ES&S machines. As the Compuware Report noted: "Results can be added multiple times due to a feature that gives an option to either add or replace the votes when uploading the results."\(^{89}\) This function can be repeatedly executed "with no warning," which would lead to over-counted votes.\(^{90}\)

This multiple counting on ES&S machines in fact occurred in the 2004 elections. In Craven County, North Carolina, 11,283 votes were added to George Bush's total as the "precinct totals [for nine of the county's twenty-six precincts] were added a second time."\(^{91}\) In Lancaster County, Nebraska, the problem of twice reading ballots "plagu[ed] almost all of the machines,"\(^{92}\) and in Sarpy County, Nebraska, as many as 10,000 "votes were counted twice."\(^{93}\)

In other cases, too few votes were recorded. Each of the

\(^{84}\) Id. at 16.

\(^{85}\) Id. at 14; DIEBOLD ELECTION SYSTEMS, supra note 59, at 15–16 (failing to contest that encryption is limited to the single DES key). For the vulnerabilities of the DES encryption standard, see DOUGLAS W. JONES, THE CASE OF THE DIEBOLD FTP SITE § 6 (2003), http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html (explaining that DES "was believed by many to be second-rate even at the time it was introduced," and that the use of DES could result in the "cracking [of] the key for one election . . . allow[ing] an attack on the data for subsequent elections").

\(^{86}\) COMPUWARE REPORT, supra note 59, at 68.

\(^{87}\) Id. at 96, 170, 203.

\(^{88}\) Id. at 181.

\(^{89}\) Id. at 105.

\(^{90}\) Id. at 129.


precincts in LaPorte County, Indiana counted only 300 votes (for a total of 22,200) even though there were 79,000 voters in the county.94 In Carteret County, North Carolina, 4,400 votes were lost, prompting a re-vote for the agriculture commissioner's race.95 And one precinct in Mahoning County, Ohio, recorded a negative 25 million votes, while a machine in a precinct in Mercer County counted only fifty-one votes for President even though 289 ballots were cast on the machine.96

e. Audit Logs

An audit log records all of the actions taken on a DRE, such as "opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access."97 Each of these actions, recorded with a time-stamp, is compiled in a report "that is a paper trail to guard against fraud."98 Despite their importance, the audit logs of each of the major vendors lack encryption.99 Not surprisingly, the Compuware testers were able to change and delete the logs,100 which would ensure that there would be "no evidence that an attack was ever mounted."101

An incident consistent with the erasing of the audit logs occurred in a September 2004 primary election in Snohomish County, Washington.102 A mysterious three and one half hour gap in the audit log appeared on the night of the election. Even though there were summary reports generated at least five times
within the period, no entries appeared in the log between 9:52 p.m. and 1:31 a.m.103

f. External Communications

The connection of DREs to unencrypted lines of communication such as the Internet only increases the vulnerabilities described above. The Compuware Report concluded that a DRE “could be compromised” if the network port it provides for loading ballot definitions and downloading and uploading vote records is “connected to an unsecured internet or intranet.”104 Similarly, the mere tapping of a phone line could have significant consequences. In particular, the intruder could “intercept votes en route to the courthouse, change them with a prewritten program, and send them on their way.”105 All of the necessary information to execute this plan appears in the source code that was posted on the Diebold Internet site. And none of the four vendors encrypt data sent over communication links.106

3. Central Tabulators

Significant flaws plague not only DREs but also the central tabulators that count the votes from each of a county’s precincts. Votes cast on DREs and optical scanners are sent by modem to the central tabulator, which counts the votes on Windows software. Diebold’s tabulators, called GEMS,107 have been used in more than thirty states and can count as many as two million votes.108

Recent investigation showed that the GEMS central tabulators are highly subject to vote manipulation. In particular, an attacker could, within a few seconds, “enter[] a 2-digit code in

104 COMPUWARE REPORT, supra note 59, at 78.
105 Zetter, supra note 57. A phone line could be tapped by “climb[ing] a telephone poll or go[ing] down a manhole and put[ting] alligator clips on the wire.” Id.
106 COMPUWARE REPORT, supra note 59, at 58, 95, 152, 203.
a hidden location [and create] a second set of votes.”109 The attacker then could generate countywide totals that bear no relationship to the data reported from each of the precincts or “melt down an election . . . with two mouse clicks.”110

Although robust security techniques and limited access to the tabulator could minimize the likelihood of these occurrences, both conditions are absent with the Diebold system. The GEMS tabulator uses a default password, GEMSUSER, that “has been all over the Internet forever.”111 Numerous people have access to the tabulator, including county employees, Diebold employees, county database technicians, printshops, and Diebold contractors.112 And the database used by GEMS, Microsoft Access, is well-known for its lack of security.113

Nor would spot checks catch the vote switches: one of the “books” of votes could display the actual votes while another—the one used for the official count—could display the bogus votes.114 In addition, as discussed above, the audit log can be altered to erase any illegal activity.115 Even the officials who run the election would have no idea that the vote totals had been changed.116

109 Id.
110 Id. Of additional concern is the role played by Jeffrey Dean, who was hired as Diebold Vice President of Research and Development shortly before the double set of books was discovered in October 2000. Dean pled guilty to 23 counts of embezzlement (including for the “sophisticated” manipulation of computer accounting records) and presided over at least a dozen changes to GEMS before the 2000 election, with each change “retaining the new hidden vote tables.” Id.
112 Harris, supra note 108.
114 Harris, supra note 108.
115 See supra notes 97–103 and accompanying text.
116 Harris, supra note 108 (“The [Microsoft] Access database, which contains the hidden set of votes, can’t be seen unless you know how to get in the back door.”); JIM MARCH, DIEBOLD’S VOTE-TALLY SOFTWARE (2003), http://www.equalcw.com/dieboldtestnotes.html (noting that the countywide totals are pulled from one data file and the precinct-by-precinct data come from another, and that “GEMS never checks to see if the two match, or informs the GEMS console user that this is
Employee communications confirm many of these risks. One Diebold employee corroborated that he could open data files, “including the audit log,” and “alter [their] contents.”\footnote{E-mail from Ken Clark to Support (Oct. 18, 2001, 9:55:02 MST), reprinted in Alastair Thompson, Diebold Internal Mail Confirms U.S. Vote Count Vulnerabilities, SCOOP INDEP. NEWS (N.Z.), Sept. 12, 2003, at app., http://www.scoop.co.nz/mason/stories/HL0309/S00106.htm.} He further noted that the security hole has been open “for at least a decade” and that he has not put a password on the files because the ability to end-run the database has admittedly got[ten] people out of a bind . . . . Jane . . . did some fancy footwork on the .mdb file [e.g., hacked the election tallying database] in Gaston [County, North Carolina] recently. I know our dealers do it. King County[, Washington] is famous for it. That’s why we’ve never put a password on the file before.\footnote{Id.}

The Compuware Report concluded that anyone “with access to the GEMS server” could change election results.\footnote{COMPUCARE REPORT, supra note 59, at 64; see also RABA REPORT, supra note 65, at 20 (noting that the only requirement for “full system administrator privileges” is “a valid phone number for the GEMS server”).} It therefore is concerning that a Diebold field tech agent confirmed that he could access the central computer using an ordinary laptop and indicated that the GEMS tabulator was accessible through the Internet.\footnote{E-mail from Robert Chen to Support (Oct. 28, 2002, 1:30 PM), copied in its entirety in MARCH, supra note 116.} Nor does it inspire confidence that the phone numbers allowing optical scan machines to contact the GEMS tabulators are “known to . . . the Diebold support staff.”\footnote{MARCH, supra note 116.}

In short, tampering with the central tabulator that counts millions of votes is astonishingly easy.\footnote{For an example of access to the central tabulator, see Bev Harris, Money, Access, and Stunning Security Flaws—A Poor Recipe for Fair Elections, SCOOP INDEP. NEWS (N.Z.), Apr. 2, 2004, http://www.scoop.co.nz/stories/H0404/S00024.htm (indicating that in a 2004 county supervisor election in Riverside County, California, one candidate received progressively more votes—allowing him narrowly to surpass 50 percent and avoid a runoff election—after Sequoia employees began accessing the central tabulator).} It could be done quickly, with no trace of the activity,\footnote{The inability to trace the activity is, in part, a consequence of the nature of digital media. See Harris, supra note 108 (documenting ability to alter audit logs “without leaving a trace”).} and with the involvement
of only a few. The types of fraud possible on DREs and central tabulators thus present significant threats to the accurate counting of the vote.

D. Partisan Affiliations

These vulnerabilities take on added concern in light of the ties that most of the major voting machine vendors have with the Republican Party. The chief executive of Diebold, for example, has been an active Republican fundraiser who famously promised "to help Ohio deliver its electoral votes to the President." ES&S was initially funded by Howard Ahmanson, a member of the right-wing Council for National Policy and the Christian Reconstructionist movement, and is partly owned today by Republican Senator Chuck Hagel of Nebraska. The parent company of Sequoia is a partner of the Carlyle Group, which has employed former President George H.W. Bush as senior advisor. And a significant investor in Hart Intercivic is Tom Hicks, who bought the Texas Rangers from President George W. Bush in 1999.

---

124 March, supra note 116 (noting that as few as five or (more likely) seven or eight people would need to be involved: "[t]wo or three programmers, one or two managers who are politically savvy and know which races to hack, one guy back in the 'build room' setting GEMS boxes up, and one guy able to collect the data from the field regarding phone numbers [and] passwords").


128 Harris, supra note 32, at 79. A survey of campaign contributions found that several of the companies gave to both the Republican and Democratic parties. The Business of Elections, ELECTION REFORM BRIEFING (Electionline.org, Wash. D.C.), Aug. 2004, at 5, http://www.electionline.org/Portals/1/Publications/The Business of Elections.pdf. Other than Diebold's contributions to the Republican party, however, the amounts were de minimis, thus not overcoming the links noted in the text. Id. at
It also is concerning that the concentration of vendors is significantly higher today than it has historically been. Two companies, Diebold & ES&S, have counted approximately eighty percent of the votes cast in U.S. elections in recent years.\(^{129}\) By reducing the number of systems that need to be compromised, such developments make it easier to commit widespread tampering.\(^{130}\)

The dangers of such concentration and party affiliation are exacerbated by the lack of transparency in vote counting today. The voting machine vendors refuse to allow inspection of the software used to count the vote, and the computerization of the process means that local election officials can no longer uncover fraud by examining the machines. As a result, the officials rely more heavily on, and often develop close relationships with, the vendors.\(^{131}\) These relationships may play a role in the enthusiasm for electronic voting displayed by Democratic and Republican officials alike.\(^{132}\) A final concern in the vote counting

\(^{129}\) 2004 U.S. Presidential Election Controversy, supra note 126.

\(^{130}\) FISCHER, supra note 2, at 13.


\(^{132}\) David Cho, Fairfax Judge Orders Logs of Voting Machines Inspected, WASH. POST, Nov. 6, 2003, at B01 (indicating that the Democratic Fairfax County (Virginia) election supervisor Margaret Luca stated that electronic voting machines “get an A-plus” even though a narrowly defeated school board candidate lost one out of every 100 votes and the county Republican committee issued a critical report that concluded that “[t]he Fairfax experience was a bitter disappointment—at best” (referencing FAIRFAX COUNTY REPUBLICAN COMMITTEE, OPERATION BALLOT INTEGRITY 2 (2004), available at http://www.fairfaxco-gop.org/download/ballot_integrity.pdf)); Lou Dobbs Tonight: Bush and Kerry Trade Jabs (CNN television broadcast Mar. 8, 2004), transcript available at http://transcripts.cnn.com/TRANSCRIPTS/0403/08/ ldt.00.html (documenting that Republican Florida Secretary of State Glenda Hood stated that she has “had no problem whatsoever” with electronic voting); see also Jason Miller, E-Voting Debate: Paper or No Paper, GOV'T COMPUTER NEWS, June 7, 2004, available at http://appserv.gen.com/23_13/state/local/26086-1.html (noting Democratic Maryland Election Administrator Linda Lamone’s statement that “[w]e have used electronic voting equipment for 30 elections, and we haven’t had a single problem with the equipment”); Dave Williams, Cox Gets Ready for 2006, GWINNETT DAILY POST (Ga.), Apr. 17, 2005, available at http://www.cathycox.com/news/4-17-05.htm (noting that Democratic Georgia Secretary of State Cathy Cox was instrumental in introducing statewide electronic voting in 2002). Another reason for officials’ enthusiasm likely is their reduced
process involves the partisan connections of many election officials themselves.\(^{133}\)

II. 2004 ELECTION

Evidence from the 2004 election is consistent with the errors and fraud discussed in Part I. This section first examines inaccuracies from the election and then presents circumstantial evidence that has been marshaled in evaluating the accuracy of the results.

A. Inaccuracies

With the exception of paper ballots, each of the voting technologies used in the 2004 election suffered from an array of errors.\(^{134}\) Several voters using punch cards had difficulty punching holes, saw pre-punched holes, and suffered from miscounted votes.\(^{135}\) On many lever machines, the levers were responsibilities in administering a paperless system.

\(^{133}\) For example, state election officials often serve as chairs of their political party’s election campaigns. Letter from Kenneth Blackwell, available at http://rawstory.rawprint.com/105/blackwell_campaign_letter2_105.php (last visited July 23, 2005) (documenting that Ohio Secretary of State Kenneth Blackwell thanked supporters for “helping deliver” Ohio and announcing that he was “truly pleased” to announce Bush’s victory in the state).

Nor are the concerns limited to state election officials. Congressman Peter King (R-N.Y.) justified his statement in the middle of Election Day 2004 that “the election’s over [and we won]” by explaining: “It’s all over but the counting and we’ll take care of the counting.” Posting of Free Press Int’l to eBlogger, Video clip: And We’ll Take Care of the Counting, http://www.freepressinternational.com/pete.999880.ny.129501.html (Dec. 5, 2004).

\(^{134}\) Thanks to the creation of an “Election Incident Reporting System” by Verified Voting Foundation and Computer Professionals for Social Responsibility, voting problems were instantaneously tracked from across the nation. These records are now memorialized in a database of more than 40,000 election incidents, including more than 2,200 associated with voting machines. DAVID DILL & WILL DOHERTY, ELECTRONIC VOTING SYSTEMS (2004), available at http://www7.nationalacademies.org/cstb/project_evoting_vvf.pdf.

\(^{135}\) See, e.g., Election Incident Reporting Number [hereinafter EIRN] 33495, 54500 (reflecting difficulty punching hole for Kerry), 60406 (reflecting difficulty punching hole for Kerry), 35414 (pre-punched holes for Bush), 48820 (pre-punched holes for Bush), https://voteprotect.org/index.php?display=EIRMapNation (follow “Download Incidents” hyperlink to view incidents) (last visited July 23, 2005); see also Dan Harrie & Mark Edington, 33,000 Ballots Lost in Shuffle, SALT LAKE TRIB., Nov. 13, 2004, at A1 (noting that 33,000 straight-party ballots of the roughly 150,000 ballots cast in a Utah county were not included in the initial tally); Robert Morgan, Waiting in Wichita, TIMES RECORD NEWS (Tex.), Nov. 4, 2004, available at http://www.votersunite.org/article.asp?id=3690 (revealing that a software “glitch” was responsible for more than 25% of the first 26,000 ballots tabulated in a Texas
broken.\textsuperscript{136} And optical scan machines malfunctioned,\textsuperscript{137} incorrectly tabulated voters’ choices,\textsuperscript{138} and even subtracted votes for John Kerry in one state.\textsuperscript{139}

But the most frequent and most severe errors were associated with DREs. The machines, which lacked the ability to conduct recounts in nearly every state,\textsuperscript{140} broke down,\textsuperscript{141} lost votes, added votes, switched votes, and suffered other problems during the 2004 election. To cite only a few examples:

- Machines in Broward County, Florida began counting backwards when they reached 32,767 votes.\textsuperscript{142}
- A DRE in Carteret County, North Carolina lost more than 4,500 votes when 7,537 votes were cast but the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{136} EIRN, supra note 135, 33002, 40706, 51331 (NY and PA counties with broken Kerry levers); see also id. at 31440, 37924, 39712 (PA counties in which levers for other Democratic candidates broken).
\item \textsuperscript{137} EIRN, supra note 135, 1087, 1118, 17647, 28659, 29326, 29404, 29577, 30200, 30673, 30709, 30710, 30718, 31402, 31406, 31930, 31939, 32042, 32096, 32451, 33143, 33164, 33641, 34478, 35985, 38687, 37106, 40367, 40674, 41187, 41339, 42451, 43540, 44797, 49025, 52056, 53974, 54456, 55204, 56181 (providing examples from AL, AZ, CA, CO, DC, FL, IL, KS, MA, MI, NC, OH, SC, TX, and VA).
\item \textsuperscript{138} For example, optical scan machines in Indiana counted straight-party Democratic tickets for Libertarian candidates. See Pam Tharp, Elections, PALADIUM-ITEM (Ind.), Nov. 23, 2004, at 12A.
\item \textsuperscript{139} Even though John Kerry led after seventy percent of the vote had been counted in fifty-seven of Oklahoma’s seventy-seven counties, he wound up losing every county in the state, with his vote totals in some counties less than they had been at the seventy percent mark. Bob Nichols, Update: Voting Machines Count Backward in Okla., OKLA. INDEP. MEDIA CENTER, Nov. 27, 2004, http://okimc.org/newswire.php?story_id=344 (noting that, in the final thirty percent of the count, Kerry lost 37,982 votes while Bush gained 393,825 votes); see also Kelly Kurt, Voters Look to Moral Issues, TULSA WORLD, Nov. 3, 2004, at A10; CNN.com Election Results (July 22, 2004), http://www.cnn.com/ELECTION/2004/pages/results/states/OK/P/00/county.000.html.
\item \textsuperscript{140} Only Nevada used DRE machines that were attached to printers. Press Release, Nev. Sec’y of State, Secretary of State Heller Announces Direct Recording Electronic Voting Machine Choice (Dec. 10, 2003), http://secretaryofstate.biz/press/121003.htm.
\item \textsuperscript{141} See, e.g., DILL & DOHERTY, supra note 134, at 3 (citing forty-two reports of total breakdowns in New Orleans); Report Shows Problems with Montgomery Voting Machines, WTOP NEWS, Mar. 31, 2005, available at http://www.wtopnews.com/index.php?sid=440855& nid=25&template (noting that fifty-eight DREs in Maryland failed to boot up); EIRN, supra note 135, 41693, 55533 (reporting breakdowns in Maryland and Florida).
\item \textsuperscript{142} John Murawski, Broward Vote-Count Glitch a Cinch for Cyber Solvers, PALM BEACH POST, Nov. 14, 2004, at 1C (noting that the flaw plagued two elections in Broward County and one in Guilford County, North Carolina).
\end{itemize}
\end{footnotesize}
machine was set at a capacity of 3,005 votes.\textsuperscript{143}

- A precinct in Mahoning County, Ohio recorded a negative 25 million votes.\textsuperscript{144}

- George Bush received 4,258 votes in a precinct in Franklin County, Ohio in which only 638 voters cast ballots.\textsuperscript{145}

- More than 11,000 votes were added to Bush's total in Craven County, North Carolina as votes for at least 9 of the county's precincts "were added a second time."\textsuperscript{146}

- There were numerous instances of votes being switched from one candidate to another. To pick just a few typical examples:

  - A voter in Broward County, Florida asserted: "At [the] review screen, [my] selection changed from Kerry to Bush 'before my eyes.'"\textsuperscript{147}
  
  - A voter in Pinellas County, Florida stated that "touch screen voting machin[es] are defaulting to Bush/Cheney" and that even though voters have "tried to change [their vote] to Kerry, [it] kept going back to Bush."\textsuperscript{148}
  
  - A voter in Palm Beach County, Florida "[t]ried 9-10 times" to cast a vote, each time deleting the machine's selection of Bush.\textsuperscript{149}

Of particular concern, nearly all of the vote switches were in one direction. My exhaustive search of the election incident database— which included every incident in which a voter called the hotline and mentioned the term "Kerry," "Bush," "Democrat," or "Republican"—uncovered ninety-nine incidents of vote switching. Of these, voters reported seventy-nine incidents of switches from Kerry to Bush, with many mentioning multiple occurrences,\textsuperscript{150} and nineteen occasions of switches from Kerry to

\textsuperscript{143} Jannette Pippin, Early Votes in Carteret County, N.C., Are Permanently Lost, Machine Maker Says, DAILY NEWS (N.C.), Nov. 9, 2004.

\textsuperscript{144} Untangling the Voting Controversies, supra note 96.


\textsuperscript{147} EIRN, supra note 135, 55055.

\textsuperscript{148} EIRN, supra note 135, 33258.

\textsuperscript{149} EIRN, supra note 135, 39396.

\textsuperscript{150} EIRN, supra note 135, 48010 (Cal); 13490, 16735, 17826, 18569, 18688, 22524, 24179, 31377, 33258, 38533, 38775, 39328, 39936, 39531, 39721, 41745,
a third party candidate. Only one voter reported a DRE switching a Bush vote to Kerry. It also is concerning that more than one-half of all reported switches occurred in the “swing” state of Florida.

Of course, a total of ninety-nine incidents does not provide a sample size to which we can attribute statistical significance, and it is at least conceivable that Kerry voters were more likely to report problems in voting. On the other hand, in thousands of precincts, Democratic and Republican voters alike had access to the election hotline phone number. And it is possible that the reported incidents are only the tip of the iceberg given that many voters would tend not to report problems after voting and that many incidents revealed multiple switches or machines that “ha[d] been doing that all day.”

Consistent with machines repeatedly making the same error is the pattern of vote switches in various states. Of the fifty-three reported switches in Florida, forty-three were from Kerry to Bush (with nine from Kerry to other candidates). Of the

42578, 43451, 44658, 46528, 47099, 48269, 52639, 53430, 55055, 55066, 55396, 55458, 55485, 55842, 55860, 55978, 58116, 58213, 58328, 58329, 60432, 60756, 61244, 62068, 63812, 63816, 63846 (Fla.); 17705, 36180, 37481, 37666, 49209, 62363 (Ga.); 35481 (Kan.); 35862, 43115, 46968, 47289, 47376, 52582, 62045, 63948 (Ohio); 14216, 14754, 15252, 15336, 18033, 18957, 19315, 21981, 26586, 28858, 29306, 37893, 46164, 47873, 59747 (Tex.); 13536, 43610 (Va.); 39275, 41871, 47787 (Wash.).

EIRN, supra note 135, 39163 (Cal.); 41979, 42530, 46394, 46762, 47606, 55080, 55477, 56831, 63818 (Fla.); 33853, 35228, 35436, 42006, 45322, 59157, 59224 (N.M.); 46385 (Ohio); 40147 (S.C.).

EIRN, supra note 135, 48034 (Fla.).

See supra notes 150–52 (showing that fifty-three incidents of vote-switching were in Florida). Even enlarging the scope of the study beyond vote switches between the presidential candidates reveals a bias towards Bush. There were fifteen reported incidents of general switches between the parties, with thirteen of these incidents favoring Republicans. EIRN, supra note 135, 15928, 17640, 31509, 33406, 41725, 43999, 46179, 47278, 47570, 47683, 49986, 53724, 60384 (favoring Republicans); EIRN, supra note 135, 46108, 55744 (favoring Democrats). There were twenty-two incidents in which it was either difficult to vote for Bush or Kerry or one of the choices was pre-selected. Of these incidents, twenty aided Bush. EIRN, supra note 135, 14203, 21614, 25706, 29441, 29974, 31061, 31931, 32344, 36177, 38151, 40346, 47630, 52219, 52341, 55454, 55637, 58013, 58748, 60876, 63847 (favoring Bush); EIRN, supra note 135, 43856, 59351 (favoring Kerry). And there were nine reported instances in which DREs defaulted to or otherwise favored a party, with six of the occurrences helping Republicans. EIRN, supra note 135, 31359, 34506, 48422, 48801, 59658, 62360 (favoring Republicans); EIRN, supra note 135, 33761, 53619, 59246 (favoring Democrats).

EIRN, supra note 135, 47099 (Fla.). See, e.g., EIRN, supra note 135, 63846 (reporting that one volunteer received seventy-five calls complaining that votes for Kerry were switched to Bush).
fifteen reported switches in Texas, thirteen were from a straight-Democratic ticket to Bush, and all seven of the switches in New Mexico were from Kerry to a third-party candidate.\textsuperscript{155} In short, the overwhelming asymmetry in the direction of vote switches raises significant questions about the operation of DREs.

B. Circumstantial Evidence

The inaccuracies unearthed in the 2004 presidential election gain added significance in light of the magnitude of potential fraud, as attackers have the capability of altering thousands, if not millions, of votes on DREs and central tabulators. Moreover, because of the hidden nature of computerized counting, the ease of altering vote counts and audit logs, and the inability to conduct DRE recounts, the ability to uncover error or fraud is lower than it has ever been. Circumstantial evidence thus is of unique importance in corroborating the accuracy of the vote count. This section explores exit polls, pre-election polls, and activity in Ohio that raises questions and serves as an independent check—typically the only one—on the vote count.

1. Exit Polls

Of all the anomalies of the 2004 presidential election, exit polls have received perhaps the most attention. As they sample actual voters, do not confront difficulties such as contacting cell-phone users, and are continually being adjusted, exit polls have generally been considered to be the most reliable type of polls.\textsuperscript{156} Since their invention several decades ago, exit polls have successfully predicted the outcome of thousands of races.\textsuperscript{157}

It therefore is not surprising that the Bush administration

\textsuperscript{155} For documentation of the switches in Florida, Texas, and New Mexico, see supra notes 146–52.


helped to pay for exit polls during recent elections in the former Soviet republics of Belarus, Georgia, and the Ukraine.\textsuperscript{158} A deputy assistant secretary of state explained that exit polls constituted one of the “ways that would help to expose large-scale fraud” and “pointed to the discrepancy between exit polls and the official vote count to argue that the . . . Ukraine election was stolen.”\textsuperscript{159}

In particular, the exit polls used in the 2004 U.S. elections involved 73,000 interviews for state polls and 13,000 for a national poll, a sample “approximately six times larger than the sample normally used in high quality pre-election \[ polls.”\textsuperscript{160}

Running the operation was Warren Mitofsky, who is considered a pioneer in exit polling.\textsuperscript{161}

It therefore is concerning that the election was marked by a greater disparity between exit polls and the official vote count than has occurred in at least the past twenty years. The national exit poll posted on the CNN.com website on November 3 at 12:23 A.M. is the most independent and accurate of all the exit polls; in contrast to the polls released throughout Election Day, it includes interviews from the entire day, and, because subsequent polls are “adjusted” to mirror the official vote count, it is the most recent poll available that can serve as an independent check on the vote count.\textsuperscript{162} The poll indicated that John Kerry received 51% of the vote and George Bush received 48%.\textsuperscript{163} In contrast,
the actual vote count favored Bush, 50.9% to 48.1%, resulting in a 5.8% discrepancy with the exit polls. Statisticians have agreed that such a disparity cannot be attributed to chance. This trend also occurred in the “battleground states,” as ten of the eleven states witnessed an official margin for Bush that exceeded—often by a significant amount—the predicted margin.

The exit pollsters, Edison and Mitofsky, have conceded that “the precinct samples did not contribute to the error of the exit poll estimates.” They also conceded that the primary source of the error is “within precinct error” (WPE), or the difference between the official and exit poll results in sampled precincts. This figure, which the pollsters calculate at 6.5%, “is the largest WPE that [they] have observed on a national level in the last five presidential elections.”

In addition, in contrast to the 1996 and 2000 elections, in which the errors were “more random,” the errors in the 2004 election were “much more in one direction.” The discrepancy

---

165 US COUNT VOTES, supra note 162, at 3 & n.3 (noting that statisticians have estimated the probability of such a disparity being attributed to chance at 1 in 1,240 to 1 in 16 million).
166 STEVEN F. FREEMAN, THE UNEXPLAINED EXIT POLL DISCREPANCY 2 tbl.1.1 (2004), available at http://center.grad.upenn.edu/center/get.cgi?item=exitpollp. The battleground states—which were listed “on at least two of three prominent lists: Zogby, MSNBC, and Washington Post”—are Colorado, Florida, Iowa, Michigan, Minnesota, Nevada, New Hampshire, New Mexico, Ohio, Pennsylvania, and Wisconsin. Id. at 2 & n.5. In the critical states of Ohio, Pennsylvania, and Florida, for example, the vote count differed from the exit polls by 2.1% to 6%, in each case favoring Bush. See NEP Declared Errors Excel Spreadsheet, http://www.exitpollz.org/tables/NEPdeclaredErrors.xls (last visited July 23, 2005) (indicating that in Ohio, Kerry garnered 53.2% in the exit polls, but received 48.7% of the vote; in Florida, he polled 49.2% but received 47.1%; and in Pennsylvania, he polled 56.9% but received 50.9%).
167 EDISON MEDIA RESEARCH & MITOFSKY INT’L, supra note 163, at 28.
168 Id. at 31; see generally US COUNT VOTES, supra note 162, at 6 (defining WPE).
170 Id. at 34.
occurred in almost all precincts, including heavily Republican precincts (those in which Bush received at least eighty percent of the vote), where the mean WPE was 10.0.\textsuperscript{171} Finally, the pollsters conceded that the discrepancy was limited to the presidential election; the error rate in the 2004 Democratic primaries, for example, was significantly lower at 1.9\%.\textsuperscript{172}

The primary hypothesis that has been proffered for the discrepancy is that more Kerry voters than Bush voters participated in the exit polls. The contention is that Democratic voters were more willing to talk to pollsters than were Republican voters.\textsuperscript{173} While such a scenario is not impossible, Edison and Mitofsky did not offer any evidence to support their hypothesis. In fact, to the extent their report offers any evidence on this point, it appears to be more consistent with the opposite conclusion: More voters in highly Republican precincts (56\%) responded to the exit poll interviews than did voters in highly Democratic precincts (53\%).\textsuperscript{174}

In short, the largest and most one-sided discrepancy between exit polls and vote tallies in the modern era cannot be attributed to sampling error or to any other documented flaw. The most likely explanation, then, is that the vote count itself was incorrect.

2. Incumbent Performance in Pre-election Polls

In the past fifty years, the pre-election polls have been an "extraordinarily accurate predictor" in forecasting the percentage of the vote that the incumbent president would receive on Election Day.\textsuperscript{175} For example, of the four incumbent presidential elections in the past quarter century (with examples from prior years detailed in the margin),\textsuperscript{176} the incumbent exceeded his final

\textsuperscript{171} Id. at 36.
\textsuperscript{172} Id. at 26.
\textsuperscript{173} Id. at 4.
\textsuperscript{176} See Gallup Poll Accuracy Record, http://www.gallup.com/poll/content/?ci=1258 (last visited July 23, 2005) (showing that in 1956, the final Gallup pre-
poll number only once (and then, by only one point). In 1980, Jimmy Carter received 42% in the final polls and 41% of the actual vote; in 1984, Ronald Reagan exceeded his performance in the final polls by 1% (59% to 58%); in 1992, George Bush’s vote totals matched his final polls at 37%; and in 1996, Bill Clinton received 51% in the final polls but only 49% of the vote.177

“On average,” one recent survey concluded, “the incumbent comes in half a point below his final poll result.”178 In contrast, the challenger “exceed[s] their final poll result by at least 2 points, and the average gain is 4 points.”179 Another recent analysis demonstrated that in twenty-eight surveys of presidential elections, the challenger received 86% of the late-breaking undecided vote.180 The reason is clear: Undecided voters often do not believe that the incumbent deserves to be re-elected but are not familiar enough with the challenger to publicly state their preference in pre-election polls.181

The 2004 elections diverge from this pattern more than any other election in the past half-century. The average of the pre-election polls pegged George Bush at 48.9% and John Kerry at 47.4%.182 Although the exit polls, which favored Kerry 51–48%, are consistent with the historical trend of Bush receiving no more than 49%, the vote tallies, which Bush won, 51–48%, are not.183 Thus, for the first time in more than a half-century, the incumbent president significantly exceeded his final pre-election poll numbers. This result is even more surprising given the high turnout in the election, a factor that has historically benefited

177 Molyneux, supra note 175. These pre-election poll numbers represent “an average of the final surveys conducted by the three major networks and their partners.” Id.
178 Id.
179 Id. (emphasis omitted).
181 Molyneux, supra note 175.
183 See supra notes 156–60 and accompanying text.
Democrats.  

Curious patterns emerge on the state level as well. Although there are many examples, I focus in this section on the events transpiring in Ohio.  

3. Ohio: Phantom Votes, Undervotes, Unusual Turnouts, and Preordained Recounts

In the aftermath of the 2004 election, many disturbing details emerged about what occurred in Ohio, such as a shortage of voting machines in Democratic areas, the restricted use of provisional ballots, challenges to minority and urban voters, misinformation, and intimidation. Although each of these likely affected the vote count in some way, I focus in this section on the discrepancies in which the voting machines played a direct role: “phantom votes,” undervotes, unusual turnout figures, and preordained recounts. Most of the reported problems occurred on punch card machines and DREs.

First, several precincts reported “phantom votes,” or more votes than voters. George Bush received 4,258 votes in a precinct in Franklin County, Ohio in which only 638 voters cast ballots. Two precincts in Perry County reported at least 124% turnout. And in Trumbull County, there were 580 absentee votes that could not be traced to voters.

Second, there were 93,000 undervotes in Ohio, with 75% more of these occurring in Democratic than Republican precincts. A machine in Mercer County counted only fifty-one votes for President even though 289 ballots were cast on the machine, and a machine in Youngstown County appeared to

---

184 FREEMAN, supra note 166, at 1 n.3.
185 For another example, see Warren Stewart, What Are They Hiding in New Mexico?, SCOOP INDEP. NEWS (N.Z.), Jan. 19, 2005, http://www.scoop.co.nz/stories/HL0501/S00152.htm (noting that more than 21,000 ballots—triple the margin separating the candidates—did not record a vote for President and that there were more than 2,000 “phantom votes” in which the number of votes exceeded the number of ballots cast).
187 McCarthy, supra note 145.
188 PRESERVING DEMOCRACY, supra note 156, at 60.
190 PRESERVING DEMOCRACY, supra note 156, at 70–71.
default to a blank screen when voters selected John Kerry, which likely would explain a 14% undervote rate in a precinct in which Kerry was receiving more than 90% of the vote. Finally, a machine in Mahoning County initially recorded a negative 25 million votes.

Third, voter turnout figures revealed unusual patterns across the state. In Franklin County (which includes urban Columbus), voter turnout figures were almost ten percent higher in the precincts that Bush won than in those won by Kerry. In pro-Kerry Cleveland, where thousands of voters waited in line for hours to vote, precincts registered turnouts as low as 7.85, 14.59, 20.07, 21.43, and 22.31%. And in ten counties, a little-known and underfunded Democrat State Supreme Court candidate received substantially more votes than the Kerry-Edwards ticket.

Nor were the anomalies limited to these forms. Warren County issued a “lockdown” and barred outsiders from observing the counting of the vote in response to a terrorist threat that the FBI denied issuing and that county officials had been planning for almost a week. In the final tally in the county, Kerry received the exact same percentage (28%) that Al Gore had received in 2000, even though he more vigorously contested the vote and benefited from independent groups expending more resources and Ralph Nader’s not being on the ballot.

As another example, Miami County reported two sets of returns: the first tally was approximately three-quarters of the total from the 2000 election; the second witnessed a vote percentage for Kerry that was, to the nearest one-hundredth of

---

193 Untangling the Voting Controversies, supra note 96.
196 PRESERVING DEMOCRACY, supra note 156, at 54.
197 Id. at 49–50.
198 Id. at 50–51.
one percent, exactly the same as it was in the first set of returns (33.92%) and a margin of victory that was precisely 16,000 votes.\textsuperscript{199} Precincts in the county reported turnouts as high as 94.27 and 98.55%.\textsuperscript{200} Finally, third parties received an abnormally high number of votes in at least ten precincts in Cleveland, such as one that had cast eight votes for third party candidates in the 2000 election, but cast (in addition to 290 votes for Kerry and 21 for Bush) 215 votes for Constitution Party candidate Michael Peroutka.\textsuperscript{201}

Fourth, the recounts suffered from a number of deficiencies. Recounts in Ohio require county boards of elections initially to compare a hand count with the machine count for a three percent sample of the votes.\textsuperscript{202} If there is a discrepancy, the entire county must be counted by hand; otherwise it can be recounted by machine.\textsuperscript{203} In violation of these rules, many county boards of elections did not randomly select the precinct samples\textsuperscript{204} and others failed to undertake a full recount even when the initial hand and machine counts did not match.\textsuperscript{205}

Also disturbing was the role in the recount played by vendor Triad GSI, whose program tallying punch-card votes was used in forty-one of Ohio's eighty-eight counties in the election.\textsuperscript{206} In Hocking County, for example, an elections official explained in an affidavit that an employee of Triad came to the county board of elections “to check out [the] tabulator [and] computer.”\textsuperscript{207} He then went to the computer that was being used for the recount

\begin{thebibliography}{100}
\bibitem{200} Id.
\bibitem{201} \textsc{Preserving Democracy}, supra note 156, at 55–56; see also Juan Gonzalez, \textit{Ohio Tally Fit for Ukraine}, \textsc{Daily News} (N.Y.), Nov. 30, 2004, at 22.
\bibitem{202} See \textsc{Preserving Democracy}, supra note 156, at 21 & n.61.
\bibitem{203} Id. at 21.
\bibitem{204} See \textsc{Preserving Democracy}, supra note 156, at 92–93 (noting that samples were not randomly selected in Allen, Clermont, Cuyahoga, Morrow, Hocking, Medina, and Vinton counties).
\bibitem{205} Id. at 94–95 (noting such activity in Fairfield, Monroe, and Lucas counties).
\bibitem{206} \textit{Ohio Election Workers Scrutinize Ballots to Determine Voters' Intent}, \textsc{St. Louis Post-Dispatch}, Dec. 16, 2004, at A04; see also \textsc{Preserving Democracy}, supra note 156, at 86–87. Also of concern is that the Rapp family, which founded and controls Triad, has been a consistent contributor to the Republican Party. \textsc{Preserving Democracy}, supra note 156, at 86–87.
\end{thebibliography}
and announced that "the battery... was dead and that the stored information was gone," and that "he could put a patch on it and fix it."208 The employee took apart the computer that was being used for the recount, "asked... which precinct and the number of the precinct we were going to count... [and then] went back into the tabulation room."209 Before leaving, the Triad employee urged the election officials to "post a 'cheat sheet' on the wall... so the count would come out perfect and we wouldn't have to do a full hand recount of the county."210 Triad officials intervened in the recounts in several other counties, with one official admitting to altering tabulating software in at least six counties.211

In short, given the ease, potential magnitude, and lack of transparency of fraud in the computerized recording and counting of the vote, circumstantial evidence is more important than ever. After examining the exit polls, pre-election polls, and occurrences in Ohio, it is clear that circumstantial evidence raises significant questions concerning the accuracy of the vote count in the 2004 elections.

III. RECOMMENDATIONS

As Part II showed, there are considerable problems with the counting of the vote in the United States today. This section offers recommendations that would dramatically improve the accuracy, integrity, and transparency of the vote counting process. The majority of the recommendations focus on the technology that is in most dire need of improvement: electronic voting.

First, and most important, is the need for legislation requiring voter-verified paper ballots for DREs. Although many states have recently enacted such legislation,212 Congress must act to ensure that every state requires an audit trail.213

---

208 Id.
209 Id.
210 Id.
211 PRESERVING DEMOCRACY, supra note 156, at 81.
As the 2004 election showed, the absence of a paper trail precludes recounts and prevents scrutiny of phantom votes, undervotes, suspicious voter turnouts, and disappearing votes. Redoing elections—as was recently done in North Carolina because of the disappearance of votes—should not be the primary option that it is when we lack the capability to conduct recounts. Nor should voters be forced to rely on vendors’ assertions that elections run “flawlessly.” Considering the documented vulnerabilities of DREs and their susceptibility to switched, deleted, and added votes, the inability to verify the vote is unjustifiable.

One potential technology that could provide an audit trail involves cryptography. For example, the company VoteHere has invented a technology that gives voters an encrypted receipt that allows them to verify that their ballot was counted. It also envisions a verification of the vote count through a randomization algorithm. Such a system holds the promise of not only allowing recounts but also verifying the accuracy of the initial counting of the vote. Despite its promise, however, it is extremely complex, not yet widely understood by computer science researchers, and not transparent to the typical voter.

For that reason, the best choice currently is a paper trail. A paper trail offers advantages not provided by other technologies. Paper offers a permanent record, allows voters to verify the contents of the ballot without relying on a computer, and provides understandable procedures for poll workers and voters.

---

214 See supra note 95 and accompanying text.
215 See, e.g., Amy Morenz, Electronic Voting Divides County Political Leaders, Sept. 20, 2004, available at http://votersunite.org/article.asp?id=2848 (quoting Diebold spokesman David Bear, who stated: “The system has performed flawlessly; there has never been a factual security issue . . . after hundreds of elections”).
218 David L. Dill, Electronic Voting: An Overview of the Problem, VERIFIED VOTING FOUND., Apr. 18, 2005, http://www.verifiedvotingfoundation.org/article.php?id=5731; see also Rebecca Mercuri, Electronic Voting, http://www.notablessoftware.com/evote.html (last visited July 23, 2005) (“Many vendors and some scientists believe that an audit trail of electronically recorded ballots can be made secure (possibly through encryption . . .), but no such systems have yet been validated through rigorous mathematical proofs, nor can they be independently confirmed for correctness by non-technical poll workers, election officials or ordinary citizens.”).
(all while not preventing voters with disabilities from voting).  

Fully ninety-five percent of the members of the largest professional organization of computer scientists agreed with the statement that DREs must provide a physical record of the vote.

One version of a "paper trail" involves a DRE that produces a paper ballot that appears under glass and is deposited into a lockbox after being reviewed by a voter. During the 2004 presidential election Sequoia DREs allowed voters in Nevada to utilize such a technology. Other examples of DREs with voter-verified paper records include the Avante Vote-Trakker and the AccuPoll.

Second, there should be mandatory audits of the vote count. The vulnerabilities and performance of DREs reveal that it is at
least conceivable that error or fraud could affect the vote count to such an extent that the winning margin would be greater than that needed to trigger a recount. A random check of a certain percentage of ballots—regardless of the official margin of victory—would provide added assurance that the vote count is accurate. California, for example, requires a hand recount of one percent of the ballots cast in an election, and a bill recently introduced in the U.S. House of Representatives would require a recount of two percent. Requiring audits in all elections would expose errors and avoid the politicized nature of recounts in close races. And performing this task in public would offer additional benefits for bolstering confidence in the vote count.

Third, more documentation is necessary at the local level. Votes should be compiled and publicly posted at precincts before being transmitted to central tabulating computers. In particular, the number of voters should be compared to the number of ballots cast, and the official count should be cross-referenced to the posted precinct results. Such practices would reduce the likelihood of widespread fraud, such as tampering with the central tabulators. Relatedly, voting machines should not have telephone, wireless, or Internet connections and should not transmit results by modem.

Fourth, the security of the machines and software should be strengthened. Voting machines need to be protected at all times and—unlike the 16,000 DREs in Maryland that had identical locks—seals and locks on the machines must be made secure. "Chain of custody" procedures should be implemented, and audit logs listing every individual who accessed the machine should be

---

228 Alexander, supra note 45 (noting that only two states—California and West Virginia—require that computerized vote counts be publicly verified).
231 See id.
232 RABA REPORT, supra note 59, at 18 (Maryland DREs); Zetter, supra note 57 (describing dangers of leaving machines unattended).
created and retained after each election. Finally, states should ensure that the version of software used during the election matches the version that has been certified.

Fifth, the certification process itself needs to be upgraded. Most of the vote-counting software used today is tested against standards from 1990, which fail to cover many problems that have been detected in the past fifteen years. The testing of software and machines should include activity such as "parallel monitoring" and "red team attacks." Parallel monitoring would, by testing randomly-selected machines throughout Election Day to see if the test votes match the machine votes, reveal machines that are programmed to perform differently in a test setting than in an election setting. A red-team attack would involve simulations in which professionals "attempt to subvert a mock election" and would tend to illustrate vulnerabilities that might otherwise go unnoticed. Finally, the certification process must be made more transparent, so that it is not conducted in secret and not reliant on the approval and funding of the vendors.

Sixth, the software itself should be subject to public scrutiny. Because the vendors treat the voting system software as proprietary and do not allow its inspection, there is a complete lack of transparency. Voters and election officials cannot ascertain how votes are recorded or counted and cannot expose bugs or malicious code. This lack of openness is especially dangerous in voting machines, which—unlike other software—cannot trace outputs such as ballots to inputs such as voter decisions. Open source software, in contrast, would allow

234 CALTECH/MIT STUDY, supra note 17, at 72.
237 See KENNEDY SCH. OF GOVT, supra note 226, at 20.
238 See JONES, supra note 235, at 5 (explaining that DREs have been described as "black box voting systems" because "observers can do very little to assure themselves that the software and mechanism inside the voting machine performs correctly").
many experts to examine vote counting systems, which would increase the likelihood of discovering security flaws.\textsuperscript{240} To pick one example, the Open Voting Consortium is developing a PC-based open source voting machine that is intended to run on a Linux-type operating system.\textsuperscript{241} At a minimum, even if the vendors treat the user interface as proprietary, the source code for the vote recording and vote counting processes should be open.\textsuperscript{242} Enacting each of these changes would increase confidence that DREs are accurately counting the vote.\textsuperscript{243} If these changes are not undertaken, then the acute vulnerabilities of DREs would counsel against their continued use. Instead, precinct-based optical scan systems would present a more reliable option.\textsuperscript{244} Such machines provide feedback to the voter—and thus have low residual vote rates—and a built-in paper trail. They are cheaper than DREs, and some versions offer access to voters with disabilities, thus complying with HAVA.\textsuperscript{245} Of course, the

\makebox[\textwidth][c]{Machines-37753.html.}

\textsuperscript{240} KENNEDY SCH. OF GOV'T, supra note 226, at 21.


\textsuperscript{242} CALTECH/MIT STUDY, supra note 17 at 46; FISCHER, supra note 49, at 27 ("The code used for vote casting and counting can be much simpler than that needed for the voter interface," because the latter is "where innovations can provide the greatest advances in usability and other benefits for voters, and the security requirements are not as stringent."); MICHAEL IAN SHAMOS, PAPER V. ELECTRONIC RECORDS—AN ASSESSMENT § 3.2 (2004), \textit{available at} http://www.electiontech.org/downloads/Paper vs Electronic.pdf (last visited July 23, 2005) ("The author has been looking at the source codes of voting systems for over 20 years and has yet to find any significant differences in their design except possibly for the number of bugs they contain.").

\textsuperscript{243} Several bills currently being considered by Congress would satisfy many of these goals. \textit{See}, e.g., Voter Confidence and Increased Accessibility Act of 2005, H.R. 550, 109th Cong. (2005) (requiring voter-verified paper ballots, mandatory manual audits, increased security, and disclosed software); Voting Integrity and Verification Act of 2005, S. 330, 109th Cong. (2005) (requiring voter-verified paper ballots and providing that these ballots are the official ballots in the event of discrepancies).

\textsuperscript{244} Punch cards and lever machines are not preferred options because of the uniquely high residual vote rates with the former and lack of an audit trail with the latter. The use of paper ballots has continually declined in the past century, but if the suggestions I recommend for DREs are not enacted, paper ballots would provide a more reliable option.

\textsuperscript{245} See Automark Technical Systems, http://www.automarkts.com (last visited July 23, 2005) (describing system that can be used by blind, vision-impaired, limited-mobility, and non-English-speaking voters); see also Dill, supra note 218 (noting that
centralized counting of optical scan ballots introduces some of the same concerns as with DREs, but at least there is more transparency and a tangible record of the voter’s intent.

Finally, legislators and county officials should be open to new technologies. Hybrid systems that combine the speed of electronic tabulation with the reliability of paper ballots promise to remedy some of the most acute vulnerabilities of DREs. The Populex system, for example, uses a touch screen that prevents overvotes and warns the voter of undervotes. But unlike other DREs, it prints a voter-verifiable paper ballot card containing a bar code that is scanned to record and count the votes and that serves as the official ballot. The system also can be used by blind, visually impaired, and non-English-speaking voters.

CONCLUSION

Imagine, as computer scientists have recently analogized, that voters privately dictated their votes to human scribes but could not inspect the work of the scribes. Such a system would not inspire confidence because no one would know if the scribes misrecorded votes. But that is the type of system we have, with computers “designed and programmed by people who are no more reliable than [the] hypothetical scribes.”

Voters in previous generations at least could witness boxes of paper ballots suddenly materializing and could know the magnitude of the fraud based on the number of suspicious ballots. Today’s software, in contrast, is characterized by a lack of transparency, an inability to prevent vote switching and the deletion of evidence of tampering, and a far-reaching scope due to the removal of physical components of the vote count.

A voter could never know, for example, that a backdoor was used in a county’s central tabulator to alter millions of votes. Or that the ability of a few to gain access to an insecure system with passwords that have been known for years could forever

---

DREs “cost at least three times as much as optical scan systems to purchase”).

248 Id. Another similar system is the AutoMARK Voter Assist Terminal. See Automark Technical Systems, supra note 245.
249 Dill, supra note 218.
250 Id.
compromise the integrity of the vote. The fact that we have not found such backdoors does not mean they do not exist. More likely, it means that their very nature makes them less (if at all) discoverable.

And it means that the existence of circumstantial evidence such as surprising results, incorrect exit polls, and blocked recounts takes on more significance than it otherwise might. At a minimum, the mere possibility that such widespread, largely undetectable fraud could take place, together with the ease with which it could happen, warrants significantly more attention to the process of how our votes are counted today.

In the aftermath of the 2000 election, many, including Congress, viewed technology as a savior. Before assuming that role, however, electronic voting must be strengthened with a voter-verified paper trail, random audits, open source software, and the other recommendations I propose. Only then can voters have confidence that technology's promise will match its perils.