How Can We Ensure the Accuracy of Vote Counts?

http://uscountvotes.net/docs_other/dopp/AdviceReDiebolds.pdf

July 4, 2005
Updated August 11, 2005

Utah's Lt. Governor Selected Diebold E-Voting Machines Which Have Been Widely Reported since Early 2003 To Be Susceptible to Election Tampering, Do Not Meet HAVA Requirements for all Disabled Voters, and Do Not Provide a Demonstrated Method for *Independent* Recounts.

by Kathy Dopp MS Mathematics, University of Utah,
Founder, Utah Count Votes http://UtahCountVotes.org

Abstract 2
What do Computer Scientists Say about Electronic Voting? 3
Who Says Diebold machines are Easily Hacked? 4
But Aren't the Machines Tested and Certified? 6
But Can't *Logic and Accuracy* Testing Detect the Problems? 6
But if Votes were Embezzled, Won't there be Evidence to Prove It? 7
But Aren't Diebold Touch-screens Good for Disabled Voters? 8
Then Why Did Utah's Lt. Governor Select Diebold Touch-screens? 9
Have E-voting machines put the Wrong Candidates into Office? 10
Is America Wide Open to Insider Vote Embezzlement? 12
Then How Can We Ensure Accurate Vote Counts? 12
Won't We Lose Money if We Look a Gift Horse in the Mouth? 14
Conclusions 15
Best Recommendations for Trustworthy Voting Systems 16
Minimum Recommendations Needed to Use Diebold DREs 16
Florida's Experience with Diebold and E-Voting 17
Bibliography of Elections Papers Written by Kathy Dopp 18

Abstract

Lt. Governor Herbert made a decision in June 2005 to purchase Diebold DRE touch-screen voting equipment. Diebold's voting machines do not yet meet HAVA requirements for all disabled voters to vote privately without assistance and they are very costly[1]. Above all, though, these machines are untrustworthy. The security flaws of Diebold's voting equipment, which would make it a first choice for anyone who wanted to embezzle votes, have been widely reported since February 2003[2]. Of the members of the Utah Voting Equipment Selection Committee not one was an expert computer scientist who was also a voting & elections systems expert without a conflict of interest, nor was any a security expert. If Diebold's voting machines were to perform the tabulations, Utah voters would have little reason to trust their accuracy.

Some methods which are thought to ensure election integrity, such as "logic and accuracy testing", do not ensure accurate vote counts. On the other hand, methods commonly used in banking and retail applications, such as routine independent randomly selected audits of duplicate paper records, could be employed to effectively ensure accurate vote counts. *It is questionable if such an independent audit system can be built* for Diebold because Diebold has never demonstrated any system to count its paper rolls, did not provide any bid for a system for counting its paper rolls, and has never tested its voter verifiable paper rolls in any election.

The best way to ensure the accuracy of our election results, is to follow the recommendations of computer scientists and security experts who do not have conflicts of interest, and reject the purchase of Diebold DRE touch-screen voting machines. Instead Utah's counties should follow the lead of Utah County which plans to forgo HAVA[3] funds in order to ensure accurate election results and to save taxpayer monies.[4]

Diebold DRE touch-screen machines have widely known security flaws, have a history of involvement in statistically implausible election results, and are susceptible to electronic errors or failures. Although measures could be taken to ensure the accuracy of their vote counts, such measures are expensive, time-consuming, and technical. One would have to build a system to perform counts and routine independent audits of Diebold's voter verifiable paper roll record of ballots. Legal measures are needed immediately to require Diebold to divulge a public method for counting its paper rolls and additional purchases of equipment would be needed long before any election.

[1] Diebold voting machines are designed so as to make it easily for novices or experts, to embezzle votes. In addition innocent errors or electronic malfunctions can corrupt election results with no way to detect or correct miscounts.
[2] http://www.dallasvoice.com/articles/dispArticle.cfm?Article_ID=5128
[3] Help America Vote Act funds supplied by the federal government to Utah for the purchase of new voting equipment.
[4] "Utah County to Look for a Lower Cost Voting Option"
http://utahcountvotes.org/docs/HeraldArticle_UtahCounty_0425.html
"County Finds Few Options for Voting Equipment"
http://utahcountvotes.org/docs/HeraldArticle_UtahCounty.html

What Do Computer Scientists Say about Electronic Voting?

At the June 30, 2005 Carter-Baker commission hearing in Houston, TX[5], a PhD computer scientist, Dan Wallach of Rice University, TX, testified that "There is no such thing as a perfect computer program. All computer programs have bugs and we can never know when such bugs will surface."[6]

Utah's computer scientists, including those from both Brigham Young University and University of Utah, advised Utah's Election Office that:[7]

> " The current generation of electronic (DRE) voting machines are not secure, do not provide voters with a way to know that their votes are being tabulated correctly, and do not provide a mechanism for effective recounts when errors arise. As such, they represent an unacceptable technical risk, regardless of how people feel about them. The only way to effectively guard against errors is to have a redundant system for counting votes. The authors of this response strongly feel that the only technology currently available that provides this necessary redundancy is Voter Verifiable Paper Ballots (VVPB)."

Unfortunately, the Diebold touch-screen voting machines do not supply any Voter Verifiable Paper Ballots that are recommended by computer scientists. They supply merely a flimsy paper roll that preserves ballot order,[8] is not countable by ordinary election officials and may not allow for "any" independent checks of the accuracy of the electronic vote counts.

Anyone who thinks that electronic vote counts can be made accurate, recall the recent problems with the electronic vote counts of the paper punch cards in some of Utah's recent elections[9]. It was possible to recover accurate vote counts from these electronic mishaps only because we had a paper ballot available. An electronic vote counting system, without re-countable paper ballots, is a highly insecure, untrustworthy method to count votes.

There is currently no way to determine if a DRE e-voting machine has recorded votes exactly as cast.

---

[5] I attended a June 29, 2005 ElectionAssessment.org hearing in Houston, TX on the day before the Carter/Baker commission hearing which the director of the Carter Commission, Dr. Pastor, attended and invited members of our hearing to attend the Carter/Baker Hearing held on June 30, 2005. These statements were reported to me from those in attendance and will become available in the transcripts.

[6] This is particularly relevant to Diebold touch-screens without any demonstrated method of counting the paper rolls, so there would be no way to recover correct vote counts from computer glitches.

[7] Please see http://utahcountvotes.org/voting_system_advice.pdf This advice to Utah was also signed by Stanford computer scientist David Dill and by Barbara Simons, past President of the Association for Computing Machinery, the world's largest organization of computing professional and who is also a retired I.B.M. researcher.

[8] Voter anonymity is violated by this "non-shuffle-able" ballot design. Any poll worker who watches the order of voters enter the booths and has later occasion later to handle the paper rolls, might learn how people voted. In addition, the paper record is stored in the voting booth with subsequent voters where it could be tampered with or wrongly removed. This system especially disadvantages the disabled who must all vote on the one machine set up for the disabled and so their ballots are particular open to inspection. Voters using a foreign language may be similarly disadvantaged.

[9] Summit County and Utah County both had recent electronic vote count mishaps.

Who Says Diebold Machines Are Easily Hacked?

Diebold voting equipment has been studied extensively and subjected to security analysis of the source code by highly regarded professional PhD computer scientists from such universities as Johns Hopkins, Rice University, and University of California, San Diego and others.

Here is what was concluded about Diebold voting equipment in a paper written by four respected computer scientists in a July 2003 report[10]:

> *"this voting system is far below even the most minimal security standards.."*
>
> *"..voters, without any insider privileges, can cast unlimited votes without being detected.."*
>
> *"... even the most serious of our outsider attacks could have been discovered and executed without access to the source code."*
>
> *"...the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them."*
>
> *"...this voting system is unsuitable for use in a general election."*
>
> *"...we performed an analysis of the April 2002 snapshot of Diebold's AccuVote-TS 4.3.1 electronic voting system. We found significant security flaws: voters can trivially cast multiple ballots with no built-in traceability, administrative functions can be performed by regular voters, and the threats posed by insiders such as poll workers, software developers, and janitors is even greater. Based on our analysis of the development environment, including change logs and comments, we believe that an appropriate level of programming discipline for a project such as this was not maintained*. In fact, there appears to have been little quality control in the process."

---

[10] *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003. The paper is available here: http://avirubin.com/vote.pdf Authors were:

TADAYOSHI KOHNO Dept. of Computer Science and Engineering, University of California at San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA. E-mail: tkohno@cs.ucsd.edu. URL: http://www-cse.ucsd.edu/users/tkohno. Most of this work was performed while visiting the Johns Hopkins University Information Security Institute. Supported by a National Defense Science and Engineering Graduate Fellowship

ADAM STUBBLEFIELD Information Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. Email: astubble@cs.jhu.edu. URL: http://spar.isi.jhu.edu/~astubble.

AVIEL D. RUBIN Information Security Institute, Johns Hopkins University, 3400 North Charles Street, Baltimore, Maryland 21218, USA. Email: rubin@cs.jhu.edu. URL: http://www.avirubin.com.

DAN S. WALLACH Dept. of Computer Science, Rice University, 3121 Duncan Hall, 6100 Main Street, Houston, Texas 77005, USA. E-mail: dwallach@cs.rice.edu. URL: http://www.cs.rice.edu/~dwallach.

Diebold's security flaws which enable any insider to easily rig elections, were widely reported on the Internet in 2003 and 2004 and would have been seen by anyone who follows voting and elections issues.[11] One would imagine that Diebold might have fixed its widely reported security problems[12] after they were reported in early 2003, but it did not.

Since being exposed in 2003, Diebold's voting systems have remained hack-able and insecure. In 2004, voting activist Bev Harris taught Howard Dean on TV how to hack into Diebold's central tabulator and change vote counts in less than 90 seconds without leaving any trace. Anyone can find simple instructions on the Internet for manipulating vote counts using Diebold's central tabulator where its DRE vote counts are tabulated.[13]

Almost one year later, RABA Technologies LLC, MD was hired by the state of Maryland to study Diebold's voting machine machines and found that none of its earlier security problems had been fixed[14].

In May, 2005, studies of Diebold's voting systems solicited by a Leon County, Florida election official[15] show that Diebold's voting systems are set up so as to allow easy embezzlement of votes. Diebold's Op Scan voting system memory cards have an executable program that can be used to add votes for one candidate and subtract votes for another, yet they still pass all logic and accuracy testing, but do not meet FEC standards or federal law.[16]

---

11 For just a few of the available reports on Diebold's huge security flaws:
"SYSTEM INTEGRITY FLAW DISCOVERED AT DIEBOLD ELECTION SYSTEMS"
http://www.scoop.co.nz/stories/HL0302/S00052.htm
"All the President's Votes?" http://www.why-war.com/news/2003/10/14/allthepr.html
"Diebold Internal Memos Admit Voting Machine Flaws" http://www.dangerouscitizen.com/Articles/904.aspx
"State Keeping Quiet on Flaws in Machines" http://www.gazette.net/200340/montgomerycty/state/180200-1.html
"Diebold's Security Flaws Now Proven" http://phoenix.swarthmore.edu/2004-02-05/opinions/13643
"Security Researchers Discover Huge Flaws in E-voting System http://www.eff.org/Activism/E-voting/20030723_eff_pr.php
"Maryland Approves Electronic Voting Machines Despite Security Flaws"
http://www.thesentinel.com/286696744072607.php
"The Case Against the Diebold AccuVote TS http://www.cs.uiowa.edu/~jones/voting/dieboldacm.html
"Electronic Voting Security Flaws: John Hopkins Researchers Respond to Diebold Analysis"
http://foi.missouri.edu/evolvingissues/electronicvoting.html
"Hopkins, Diebold Argue Over Voting Machine Security Flaws"
http://www.washingtontechnology.com/news/1_1/daily_news/21302-1.html
"How to Rig Elections in the United States" http://www.whatreallyhappened.com/rigvote.html

12 Jul 7, 2005 Wired News Report "E-Vote Guidelines Need Work" mentions of Diebold's security flaws.
http://www.wired.com/news/evote/0,2645,68116,00.html?tw=wn_tophead_1

13 http://groups.msn.com/votefraudusa/3.msnw and http://www.equalccw.com/deandemo.html

14 This was reported in the New York Times on January 30, 2004. RABA report
http://www.raba.com/press/TA_Report_AccuVote.pdf January, 2004

15 The Leon County, FL Election Director, Leon Sancho arranged in May, 2005 for his county's Diebold voting machines to be tested by a computer security expert. See
http://www.yubanet.com/artman/publish/article_21497.shtml or
http://www.bbvforums.org/forums/messages/1954/5921.html

16 Diebold's Op Scan voting machines were found by Miami Herald recounts to have miscounted votes in both the 2000 and 2004 presidential elections.

But Aren't the Machines Tested and Certified[17]?

According to Kim Zetter of Wired News:

> The "independent testing labs," or ITAs, are private, for-profit labs that receive money from voting vendors to test their systems, giving the vendors control over such parts of the testing process as who gets to view the test results which usually remain secret. This lack of transparency means that state officials who buy voting machines seldom know about problems that occurred during testing.
>
> ITAs test the systems according to standards developed in 1990 and rewritten in 2002. But the standards, demand little in the way of security and contain loopholes that allow parts of voting systems to slip past certifiers without being tested. The labs generally test the machines for functionality but don't thoroughly examine them for rogue software that could alter votes.
>
> Once machines are tested, voting vendors constantly update the software. Until now, procedures for tracking and securing certified software have been extremely poor, so no one could ensure that the software tested was the same, unaltered, software used in elections. California encountered this problem when officials discovered that Diebold Election Systems installed uncertified software on its machines in 17 of the state's counties.
>
> The National Institute of Standards and Technology recently installed a new voting software library to address this problem, but it's unclear whether it will work in practice. The library will store checksums, which are measures used to protect the integrity of data, for certified software. Election officials can then compare their software against stored versions to ensure that it wasn't altered. But election officials plan to use the library only when an election dispute arises, not as a matter of course before elections.

But Can't *Logic and Accuracy* Testing Detect the Problems?

No amount of logic and accuracy testing can catch or detect problems that may cause voting machines to miscount votes. [18]

1. Voting machines can be thoroughly tested and found to count accurately on the day prior to an election and on the day following an election, and yet easily miscount votes only on the exact day of an election.
2. Even when randomly selected voting machines are pulled on election day for testing[19]:
    a. Is the election going to be canceled if a vote count problem is detected?

---

[17] This section taken from Wired News article "An Introduction to E-Voting" by Kim Zetter July 7, 2005 http://www.wired.com/news/evote/0,2645,68097,00.html?tw=wn_story_page_prev2 My own knowledge of the ITA certification process is consistent with everything Kim Zetter says.

[18] The ITAs (Independent Testing Authorities) that are paid to test and certify voting equipment in America have missed many crucial security and other flaws on many vendors' equipment, prior to certifying them. Thousands of votes have been miscounted or lost in known instances. It is not known how many votes have been miscounted in undetected instances.

[19] This requires extra machines to replace the ones being tested.

b. Due, in part, to the requirement for anonymity, there is often no way to correct vote counts errors that are detected.
c. Voting machines can be deliberately or accidentally set to miscount votes at some time during election day after machines have already been pulled for testing only after a certain threshold of votes is reached. [20]
d. Wireless network cards can be hidden inside video or other cards inside proprietary hardware that even competent local technicians cannot detect. These cards can be used during election day to modify vote totals in an undetectable way from vehicles parked outside polling locations.
e. Miscounts can be introduced at the central tabulator at the county election office by changing vote totals there in a few seconds.[21]
f. Miscounts can be introduced when transporting the memory cards that hold each voting machines' votes from the polling locations to the precincts by substituting memory cards, by omitting inclusion of some memory cards, or by tampering with memory cards.
g. Diebold voting equipment that was tested in May, 2005 in Leon County, FL was found to be easily rigged to add votes to one candidate and subtract votes from another, and yet it passed all logic and accuracy testing and raised no flags that local election officials could see.[22].

3. Logic and Accuracy Testing procedures for voting equipment are generally set up by Voting Machine vendors in a way so as to ensure that the equipment never fails. They are not a true test of any voting equipment. To conduct true tests of voting equipment accuracy, it is necessary to hire expert skilled testing engineers to design and conduct the tests.

In sum, it is impossible to do enough testing to detect all possible errors or manipulations that could occur. For example the testing that has been done by the ITAs (Independent Testing Authorities) which certify voting equipment have consistently missed critical flaws in voting equipment. Specifically ITA testing has missed crucial flaws in Diebold's voting equipment that are in violation of federal FEC standards for voting equipment.[23]

But if Votes Were Embezzled, Won't There Be Evidence To Prove It?

No. It is likely that no evidence will be found. The difficulty of finding evidence of vote embezzlement on an electronic voting machine after an election is three-fold:

1. Computer programs are compiled into machine language before running them and machine language is not humanly readable. The best that can be done is to create assembly language programs from the machine language. Only a few computer scientists

[20] For instance, some machine bugs have been reported that allowed only so many votes to be cast before an overflow error occurs and deliberate hacks that shift votes between candidates are only triggered after a certain number of votes were cast on election day.
[21] This is easy to do, even for computer novices. Videos available on the Internet teach any computer novice in a few minutes how to change vote counts on Diebold's central tabulator in 30 seconds or less.
[22] Refer to articles in footnotes in section "Who Says Diebolds are Easily Hacked?" and check votersunite.org or voteprotect.org for additional instances.
[23] Refer to BlackBoxVoting.org

are experts in assembly language. It may take weeks to decipher even one low level assembly language program to see what it does. Diebold voting machines are built on top of Windows, a system that needs constant upgrades to be secured and has thousands of programs and drivers, any one of which could be modified to embezzle votes. It may take six months or longer for an assembly language expert to reverse engineer one voting machine.

2. There are many ways to miscount or embezzle votes which don't leave a trace of evidence that would be revealed by the reverse engineering process described above such as:
    a. Vote miscounts in the form of malicious programs can be introduced in data files, in ballot definitions, or on memory cards that are over-written or erased from memory by the end of election day.
    b. Vote miscounts can be introduced through back-doors or security holes (some of which have been shown to exist on Diebold's machines[24]) without using any programs, or writing any log entries. There is even a video on the Internet showing how to hack into and change vote totals on Diebold's central tabulator that any computer novice can quickly master and execute in about 30 seconds.

3. Diebold's voting machines by design necessitate over-writing all evidence of prior elections with each ensuing election. In other words, to investigate Diebold's voting machines for evidence of tampering or vote miscounts, all future school board or other local elections would have to be cancelled for months or years until the evidence could be investigated about the prior election. In other words, to hold future local elections, much evidence must be overwritten that might enable detection of a fraudulent prior election. Voting machines could be easily designed to preserve information needed for investigations, but Diebold's are not.

But Aren't Diebold Touch-screens Good for Disabled Voters?

An article entitled "Diebold Touch Screens Don't Meet Disability Requirements" was released on June 28, 2005 by Susan Pynchon, news-journalonline.com
http://www.verifiedvotingfoundation.org/article.php?id=6072

On July 20, 2005 the U.S. Election Assistance Commission released a new advisory, explaining the requirements for voting machines to receive HAVA funding. Diebold touchscreens do not yet meet HAVA requirements for error rate maximums or for the disabled. Utah may have been duped into thinking that Diebold's DRE touch-screen voting equipment is HAVA-compliant as far as meeting the needs of disabled voters. However, unless Diebold offers a specific guarantee of HAVA compliance, with real penalties for failure, millions of dollars in taxpayers' money may be squandered on equipment that will have to be scrapped or retrofitted at taxpayers' expense after Jan. 1, 2006 to meet HAVA requirements for the disabled.

While the proposed Diebold touch screens may provide accessibility for the blind, they are impossible to use for people with many other types of disabilities, including quadriplegics or

[24] Refer to the footnotes in the section in this paper entitled "Who Says Diebold Machines are Easily Hacked?"

those with severe manual impairments. Where is the sip/puff feature, the foot pedal or the joy stick offered by the competing AutoMark Voter Assist Terminal that Utah's Lt. Governor decided against purchasing?

The AutoMark, rejected by Utah's Lt. Governor, was developed in concert with the disabled community and offers a full guarantee of HAVA compliance that can be incorporated into a contract with the county, thereby indemnifying the county and assuring compliance. This is not true for the Diebold DREs.

Diebold DRE touch-screen voting machines disadvantage the disabled in other ways as well.[25]

Then Why Did Utah's Lt. Governor Select Diebold Touch-screens?

Selecting any voting machine other than Diebold DRE touch-screens was a "no-brainer", so why did Utah's Lt. Governor select Diebold touch-screens for Utah?

While we may never know the motivations of the Lt. Governor, we do know that he and the overwhelming majority of the Utah Voting Equipment Selection Committee members are computer novices, and that not even one computer scientist who is a voting system expert, nor one computer security expert, was appointed to the Utah Voting Equipment Selection Committee. We also know that the committee repeatedly ignored the advice of Utah's computer scientists throughout its selection process.[26]

Diebold lobbyists were active in Utah's voting equipment decision. Diebold had five lobbyists working in Utah during Utah's selection process. Diebold's lobbyists had free access to meet with and speak to Utah's legislators, Utah's Lt. Governor, and the Utah Voting Equipment Committee members. On the other hand, ES&S, the maker of less expensive, more secure and more trustworthy electronic voting systems with paper ballots, had no lobbyists in Utah. While Diebold poured its money into lobbyists, ES&S spent its money on improving and securing its voting systems in response to advice from expert computer scientists.

It has become the pattern in America for election officials in the U.S. to be given positions with voting companies within a year or two after awarding lucrative overpriced contracts to voting machine vendors. Diebold gave a county election official $10,000 in Ohio which was donated to the Republican party, as reported by the AP, July 20, 2005.[27].

False information was spread during Utah's selection process. County Clerks among the voting equipment committee wrongly believed that optical scan paper ballots were inadequate to handle

---

[25] The disabled must use a specially outfitted touch-screen machine, which segregates the ballots as well as preserving ballot order: Thus voter anonymity is especially violated for the disabled.

[26] From July 1, 2005 to October, 2005, Utah Computer Scientists five times advised the Utah Election Office in writing regarding the selection of voting equipment for Utah, but their advice was ignored each time. The five documents are available online at http://utahcountvotes.org and are listed on the cover page of this report.

[27] Ohio is one of the states with numerous vote count irregularities, including precincts where turnout was reported to be close to or even over 100% and where researchers interviewed enough persons after the election who claimed not to have voted, to disprove the validity of the election results, and where the exit poll results showed Kerry won the presidential race, but the official election results showed that Bush won.

Salt Lake County elections[28]. These misperceptions were not revealed to the vendor of the AutoMARK and were uncovered only in the last few weeks of the selection process after public input had closed[29]. A Diebold salesperson told the Lt. Governor that the reason that Utah's computer professionals overwhelmingly supported ES&S in a public hearing was because an ES&S representative had instructed them all in exactly what to say. Utah's county clerks were told in a meeting that Kathy Dopp was being paid by ES&S to support their products.[30] Any reporter who interviewed Utah's Lt. Governor Herbert or Utah's Chief Election Officer in 2005, was misinformed about the options that Utah had available to it, and consequently there were false reports in papers like the Salt Lake Tribune, the Deseret News, and the Park Record[31]. The Lt. Governor's Chief of Staff Joseph Demma invented many unlikely false stories about Kathy Dopp which he released in an August press release.[32]

In any case, Diebold voting equipment gives unlimited ability to Utah's election officials to rig Utah's election results, easily, on the central tabulators or via more sophisticated hacks on its touch-screen voting machines.

Voting machine vendors fund some meetings and events for the U.S. Election Assistance Commission, the National Associations of Secretaries of State and the National Association of State Election Officials. At these nation-wide get-togethers, the voting machine vendors have employed skillful marketing strategies that include jokes and comments to induce election officials to discount the advice or opinions of voters, election activists, and computer experts.

Have E-voting Machines Put the Wrong Candidates into Office?

Many suspicious statistically implausible election results have been reported which were tabulated using E-voting touch-screen machines.[33] Here are some well-documented examples.

Georgia, 2002 - Georgia implemented new Diebold touch-screen voting machines in time for its November 2002 election. Opinion polls in Georgia on the eve of the 2002 general election showed Democratic incumbent Gov. Roy Barnes leading by 9-11 points and Sen. Max Cleland ahead of his Republican challenger by 2-5 points, so it was a shock on election night when the returns showed Barnes losing to Republican Sonny Perdue, 46 to 51 percent, a swing of as much as 16 points from the last opinion polls, and Cleland losing to Saxby Chambliss by 46 to 53 percent, a last-minute swing of 9-12 points. No paper ballots for recounts were available.

Nevada, 2004 - Nevada implemented new Sequoia touch-screen DREs prior to the November 2004 election. Exit polls showed that Kerry won, yet official results showed that Bush won.

---

[28] Salt Lake County Clerk Sherrie Swensen noted that her task force in 1992 found that the 14" op scan ballot available at the time, could not contain all the races for Salt Lake County.

[29] I discovered these incorrect rumors after the final public hearing from a clerk who thought that the AutoMARK could not be considered for Utah because its Op Scan ballot was too small for SLC, when the largest size two-sided op scan ballots are much larger than the largest election that Salt Lake County has ever had or plans. Op scan ballots can be designed to handle even New York's full face ballot requirement.

[30] This false rumor was spread about myself to county clerks in Utah and to at least one local reporter. County clerks are the election officials for each county.

[31] For instance, the Lt. Governor and Utah election officials always failed to inform reporters who interviewed them that there was a less expensive Optical Scan computerized voting system with a voter verifiable paper ballot available that was an option for Utah's voting equipment. The pricing for such a system was never reported.

[32] See http://utahcountvotes.org/JosephDemma.html

[33] "Is Technology Stealing Our Votes?" http://www.spiritofmaat.com/archive/jan4/diebold.htm
"Diebold Patched Georgia's Election" http://www.populist.com/03.20.dispatches.html

When the Green party tried to do a recount, they discovered that a recount would cost an estimated $400,000 and could not be performed by Nevada's own election officials. Instead the recount must be performed by the outside experts of Sequoia. A recount was never performed. Nevada's 2004 election remains under a cloud of suspicion.

New Mexico, 2004 - New Mexico counties use either Optical Scan paper ballot machines or pushbutton paperless electronic machines. In New Mexico's 2004 presidential election, the exit polls showed Kerry had won, yet the official election results showed Bush had won. New Mexico also had the highest rate of under-votes in the 2004 election of any state. According to official results, as high as 19% of voters in some precincts went to the polls on election day and yet cast no vote for president. The number of under-votes in NM's presidential race was significantly higher in counties using touch-screen electronic machines than in counties using op-scan ballot voting machines where the under-vote rates looked normal[34].

North Carolina, 2004[35] - In Raleigh, N.C. the votes of more than 4,400 people were lost in Carteret County. There was no way to recover the correct count, so the election had to be re-held.

Nebraska, 1996 - Senator Chuck Hagel[36] was elected to the U.S. Senate in the most "surprise upset of the election season" according to the Washington Post. Hagel owned the voting machine company, American Election Systems[37] which counted the votes in his own election.

Florida, 2000 and 2004 - The Miami Herald did recounts of the electronic vote counts in Florida counties using optical scan ballots, and found that enough votes shifted back to Gore and Kerry in the hand recounts that it was likely that Florida's electoral votes had been misallocated.

Unfortunately, possible vote embezzlement or innocent miscounts are difficult to detect today because:

1. Many races are decided on small margins where small amounts of vote miscounts would raise no red flags.
2. Many county and state election offices have not made the data easily available for mathematically analyzing their elections, or have made the data available but no analysis has been performed.
3. Opinion or exit polls are often unavailable.
4. Independent routine audits of voter verifiable paper ballots are not performed.

In other words, many more candidates may have been wrongly sworn into office based on fraudulent or incorrect election results tabulated by E-voting machines than available statistics indicate.[38]

---

[34] New Mexico also had 10,000 more absentee ballot votes counted than absentee ballots actually cast, but this padding of the absentee ballot votes was masked by reporting the results added together with the under-votes of machine counted election day votes, and was only discovered well after election results were certified.

35 http://www.wral.com/news/4063351/detail.html Jan 07, 2005 "Possible Voting Verification Measures Face Scrutiny"

[36] Senator Chuck Hagel is a well-liked moderate Republican Senator who continued to own stock in voting machine companies well after he became a Senator.

[37] AIS is the precursor to voting machine vendor ES&S.

[38] I have not taken the time to gather lists of known vote miscounts in prior elections tabulated on E-voting machines for this paper, but there are many from many different states and counties.

Is America Wide Open to Insider Vote Embezzlement?

For over a decade, over 95% of U.S. votes have been counted electronically and not independently audited to detect possible miscounts or protect from insider vote embezzlement. What would happen if for decades we set up our financial institutions so that insider embezzlement was easy and detecting it was very difficult, often impossible? Is this even conceivable? Yet, U.S. election systems have given free license to insiders to embezzle votes. As explained above, when vote embezzlement occurs, it can rarely, if ever, be proven.

U.S. voting systems make it easy for insiders[39] to embezzle votes to rig elections. With new electronic ballot voting machines like Diebold touch-screens that do not use paper ballots that are easy to hand count, it is easier than at any time in history to embezzle votes, put the wrong candidates into office, and escape detection.

Diebold's DRE touch-screen voting equipment's voter verifiable paper trail is difficult[40] to independently audit and can perhaps only be audited efficiently by Diebold's computer technicians.

On the other hand, the less expensive AutoMARK Op Scan system that was rejected by Lt. Governor Herbert employs paper ballots that are both machine and easily hand countable, allowing for easy independent audits of vote count accuracy.

Then How Can We Ensure Accurate Vote Counts?

1. The best option for ensuring accurate vote counts is to select a secure voting system that allows for convenient hand counts of voter verifiable paper ballots for audits. Utah should abandon the selection of Diebold DRE touch-screen voting machines. Instead it should purchase voting machines that are easily independently auditable, better for the disabled, and less expensive, that would result in shorter poll lines and be easier to administer. Counties who purchase their own superior voting equipment would save monies and be able to ensure vote count accuracy.[41]

2. Although there is no way that accurate vote counts can be ensured with these machines, *the following steps could be taken to attempt to secure our elections from vote embezzlement, innocent errors and electronic failures*:

    a. Require the voting machine manufacturer, Diebold, to provide our county, at no extra cost, the specifications and open source, public programming instructions, public bar code specifications, and anything else necessary to build equipment to independently audit its vote counts by hiring local computer technicians, including:
        i. Paper Roll Advancers

[39] voting machine vendor staff persons and election officials

[40] Diebold has never demonstrated any method of recounting its paper rolls, nor have their paper rolls been tested in any elections, and its sales persons at both the Mock Election and the Legislative Demonstration were unaware when I asked them in December 2004 of any method for performing any independent recounts, or any recounts whatsoever, of its paper roll record of votes.

[41] Lt. Governor Herbert said in a March, 2005 interview that Utah's counties may elect not to go along with the state's purchase and purchase their own voting equipment.

ii. Bar Code Readers of public, open source bar codes
iii. Public, open source program to read the bar codes
iv. Computer laptops

b. Ask to see a *working* demonstration of the voter verifiable paper rolls and a working demonstration of the ability of the paper rolls to be recounted.[42] Many brand new DRE touch-screen voting machines with a voter verifiable paper roll have been found to be *not independently auditable* by local election officials[43].

c. If our county succeeds in obtaining the necessary specifications from Diebold that would permit us to build systems to independently audit our vote counts, then our county needs to immediately purchase all the necessary equipment, and pay trusted local computer technicians to build and operate paper count systems.

d. Conduct routine independent audits in every election of the voter verifiable paper rolls in a sufficient small percentage of randomly selected precincts to give at least a 90% chance of detecting vote miscounts assuming that 5% or fewer of precincts are miscounted. Any discrepancy should trigger an automatic county-wide recount, at the county's expense.

e. Secure the electronic voting machines in a secure, dry storage facility.

f. Hire security experts to design procedures to ensure that insiders could not subvert the election by designing procedures for:
   i. Access to voting equipment
   ii. Repairs or upgrades to voting equipment
   iii. Transportation procedures for voting equipment
   iv. Securing voting equipment while in storage
   v. Access, public observers & security of the central tabulators at all times and while tallying vote totals.
   vi. Installing ballot definitions on voting equipment for each election

Designing security procedures to protect electronic voting equipment from malicious insider tampering is a challenging and perhaps impossible task. There are numerous stories, regarding Diebold and other DRE voting machines, of unauthorized software being installed immediately prior to an election and that election was then reported to have returned highly statistically improbable vote counts[44].

---

[42] No counting of Diebold's paper rolls have ever been performed in a real election and, in contrast to ES&S, no demonstration was even provided by Diebold's sales force to show that recounts of Diebold's paper rolls are possible, in either Utah's Mock Election or Diebold's demonstration to Utah Legislators.

[43] Nevada bought brand-new DRE touch-screen voting machines with voter verifiable paper rolls prior to the November 2004 election in which Nevada had a high rate of reported problems with its voting equipment as reported to the Election Incident Reporting System of VoteProtect.org. In addition, exit polls showed that one candidate won Nevada's electoral votes for the U.S. presidential race, yet its official election results, computed on the brand-new DREs showed that a different candidate won the election. A recount request by the Green party was abandoned when it was discovered that the voting machine vendor had to be hired to recount the paper record at huge expense because local election officials were unable to recount the brand new paper rolls themselves. A claim by the Nevada Secretary of State that all counties audited the voter verifiable paper roll trail has been found to be untrue by investigators.

[44] Georgia in November 2002 using Diebold DREs; Snohomish County, WA using Sequoias in November 2004; California using Diebolds in November 2002 and other elections in other states have reported the use of uncertified software, installed at the last minute prior to elections and followed by highly improbable election results.

Won't We Lose Money if We Look a Gift Horse in the Mouth?

No. Actually we would SAVE money by turning down HAVA funding for new voting equipment. DRE (digital recording electronic) voting machines are much more expensive than the electronic Op Scan paper ballot systems in many respects:

1. Initial purchase
2. Storage
3. Transportation
4. Security
5. Upgrades and Maintenance - Because Diebold's machines are proprietary, our county will be captive to Diebold's pricing for upgrades and maintenance.
6. Need for Consistent Power Supply on election day
7. Training of poll workers, voters, and election officials
8. Building the computer systems to make it possible to audit its voter verifiable paper records that are not designed to be conveniently handcountable
9. Possible legal suits by the disabled or against the vendor are more likely as has been shown already.[45]
10. More substantial voting booths needed to hold DREs.

To save money, Miami-Dade County in FL is planning to scrap its brand new DRE voting machines that it purchased with HAVA funds and spend its own taxpayer's money to replace them with an optical scan system that counts votes electronically, allows for hand recounts of paper ballots, and is friendlier for the disabled.

Utah County in southern Utah is also foregoing HAVA funds and purchasing its own optical scan system to save money and reduce the administrative complexity of its elections.

Other counties in America today who have purchased DREs are already looking at other options.

The following is a simple estimated cost comparison for just the initial cost of DREs versus Op Scan voting equipment:

Price Comparison
Sample: POLLING PLACE with FIVE (5) VOTING BOOTHS

Optical Scan	DRE
(1) Ballot Marking Device $4,500	(5) DRE touch-screen machines $3,000+/machine
(1) Polling Place Op Scanner $5,000	
Total $9,500	Total $15,000+

The above chart does not include other costs:
1. Diebold's central tabulation system for the county office
2. more expensive voting booths
3. extra optical scanning equipment at $3,000/machine that would be required to count each 5,500 absentee ballots

[45] See the Electronic Frontier Foundation EFF.org for a list of legal suits against Diebold.

4. $25/op-scan machine/year maintenance and license fee
5. the price of backup memory cards
6. roughly $50/touch-screen/year management licensing fee
7. roughly $200/hour on-line help-desk support cost
8. roughly $70/touch-screen/year maintenance cost
9. the six-unit carts for transporting the touch-screens of $360 each
10. $10,000 "ballot on demand printer".

Most importantly, the above pricing does not include, and Diebold never mentions in its bid proposals anywhere, the extra laptops, scanners, programs, and technical staffing that are required to build the systems needed to be able to independently recount the voter verifiable paper rolls in the case of a computer error or malfunction or in case the election is contested.[46]

In Utah, the state-wide savings of purchasing Optical Scan devices would be at least $10 million if it purchased the more trustworthy, more disabled-friendly AutoMARK op scan system or the AccuPoll DRE machines which print hand-countable, op-scannable paper ballots.

Conclusions

Utah's Lt. Governor would have been hard pressed to find more expensive, less trustworthy voting equipment for Utah. Diebold voting machines maximize the possibilities for vote tampering. Furthermore, no improvements appear to have been made to Diebold's voting systems since its flaws were first reported in early 2003.

The design of Diebold's touch-screen voting system, even irrespective of its technical flaws, is inherently slower in obtaining election results and less secure than the AutoMARK precinct based op scan system because no vote counts are done in the precincts. Instead, the memory cards from each touch-screen which contain the vote counts must be hand carried to the county office where they are tabulated, using the insecure, hackable Diebold central tabulator[47]. The Diebold optical scan system that counts the absentee ballots was tested by a security expert in May 2005 in Leon County, Florida, and discovered to be easily rigged to add votes for one candidate and subtract votes from another, even though it passed all logic and accuracy testing.

Some counties and states have de-certified Diebold DRE voting machines[48]. Other counties are scrapping DRE voting machines they purchased with HAVA funds and buying new op scan equipment at their own expense, to "save money". [49]

Diebold has demonstrated no method to detect or correct vote miscounts using their touch-screen voting equipment. Our county should purchase better, less expensive voting systems. If, however, our county adopts Diebolds, then we must adopt the expensive, complex methods that may permit

[46] Such a system to recount Diebold's paper rolls has never been demonstrated by Diebold, nor tested in any election. Diebold's own sales people were not aware of such a system. Diebold would have to make the plans for such a system public if its system is to be independently auditable by outsiders not within Diebold. If an electronic failure occurs, this (possibly vaporware) system would be the only way to recover vote totals.
[47] Any novice computer user can learn how to hack Diebold's central tabulator on the Internet.
[48] The state of CA de-certified Diebold touch-screen voting machines and Diebold settled a lawsuit brought against it by voting activists BlackBoxVoting.org and the state of CA. See EFF.org for other lawsuits involving Diebold
[49] Miami-Dade County plans to scrap its new DRE voting machines that were purchased with HAVA funding to buy op scan voting machines on its own dime - in order to save money. CA decertified Diebold DREs and settled a lawsuit with election activists in CA.

Diebold's voter verifiable paper roll ballot records to be counted. Diebold must demonstrate a working system and supply the necessary open source programs and information that local technicians would need in order to build the system to count Diebold's voter verifiable paper roll record of ballots. Without such a system, it will not be possible to detect and correct vote miscounts that will arise from computer glitches, innocent errors, or insider embezzlement.

The Diebold system selected by Utah's Lt. Governor does not currently meet Help America Vote Act (HAVA) Requirements for the disabled community, so that additional voting equipment, such as the AutoMARK, may have to be purchased to meet those needs.

Best Recommendations for Trustworthy Voting Systems

There is nothing more crucial to the functioning of U.S. democracy than accurate vote counts. Therefore, I strongly recommend the following steps for all election officials:

- Do not use Diebold touch-screen voting machines in our county elections. Instead, save taxpayer monies by purchasing less expensive, more trustworthy optical scan election equipment such as the AutoMARK or AccuPoll touch-screens that provide independently hand-countable voter verifiable paper ballots.

- Follow the recommendations of computer scientists who are voting system experts who have no conflict of interest.[50] The most important of these is a requirement for hand-countable voter verifiable paper ballots (VVPBs) for all elections.

- Implement routine audits of a sufficient percentage of the VVPBs in every election to ensure the accuracy of vote counts.[51]

- Publicly release the county's detailed precinct-level vote counts broken out by type of vote (election day, election day -provisional, absentee,..) immediately following every election so that independent analysts can mathematically analyze our elections to detect irregular patterns that may indicate possible vote miscounts.[52]

Minimum Recommendations Needed to Use Diebold DREs

If Diebold DRE touch-screen voting machines are used, the following minimum procedures for ensuring the accuracy of vote counts need to be followed:

- Require that Diebold guarantee that its voting machines are HAVA compliant by allowing disabled voters to vote unassisted. Make sure that real, enforceable penalties exist for failure.
- Require that Diebold *demonstrate* how to count and recount its paper rolls[53] and provide the specifications for software and hardware and open source public programming instructions and

[50] Best Practices for Electronic Voting. See http://uscountvotes.net/docs_other/dopp/Best_Practices_US.pdf was written by Open Voting Consortium computer scientists and professionals, dedicated since 2000 to designing better voting and elections systems. See openvotingconsortium.org

[51] An audit calculator is available to determine what probability of detecting at least one miscounted precinct is obtained by auditing various percentages of precincts in any county. This calculation depends on the number of precincts in the county, the assumed percentage of corrupted precincts, and the percentage of precincts that is audited. See http://uscountvotes.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf

[52] Please see http://uscountvotes.org/ucvAnalysis/US/election_officials/ElectionArchive_advice.pdf

[53] It might be nice if it were possible to count the rolls more than once without tearing the thin paper.

public open source bar codes to enable independent audits of vote counts obtained on its DRE voting machines.

- Purchase the necessary paper roll advancers, laptops, op scan equipment and technical support to build the systems for independently auditing vote counts produced by Diebold's touch-screen voting machines.[54]

- Hire competent local computer technicians to examine the voting equipment hardware prior to every election to make sure that no hidden wireless or wired network cards or other communications devices have been installed inside the Diebold voting machines that would permit remote vote tampering from outside the polling locations. This may not be possible as Diebold's hardware is proprietary and network cards can be hidden inside proprietary video or other hardware cards. This entire list may be of no avail in that case.

- Hire a known computer security expert to examine and test the Diebold DRE touch-screen voting machines for security flaws.

- Do not connect any vote casting or counting equipment to any network for any purpose, including exit poll or election results reporting.

- Perform *routine audits of the voter verifiable paper records in every election* in a large enough percentage of randomly selected precincts to ensure a 90% or greater probability of detecting vote miscounts if 5% of the precincts are assumed to have corrupted vote counts.

- At minimum, prior to implementation, city and county attorneys need to require that Diebold:

  1. Demonstrate a working system to recount Diebold's voter verifiable paper rolls.

  2. Make available open source specifications needed to enable local technicians to build a system for independently auditing Diebold's voter verifiable paper rolls.

  3. Provide a written guarantee that the Diebold DREs meets HAVA requirements for all types of disabled voters with a full refund of Diebold's fees and that judgment of violation of the guarantee be solely at the local agency's call. Diebold has been a pretty slippery company[55] so when they say, "Guarantee? Sure!" nail them down so they understand that non-performance equals real penalties. If this is not possible, purchase differentl voting equipment for the disabled or prepare for possible lawsuits from the disabled community for not meeting HAVA vote act requirements.

- Publicly release our county's detailed precinct-level vote counts broken out by type of vote (election day, election day -provisional, absentee,..) immediately following every election so that independent analysts can mathematically analyze our elections to detect irregular patterns that may indicate possible vote miscounts.[56]

Florida's Experience with Diebold and E-Voting

[54] It is uncertain whether or not this is even possible to do without first having Diebold produce the systems and programs for building such a system and making them publicly available with a guarantee to keep them publicly available and a working demonstration to show that it works.
[55] California has had lots of experience with Diebold. Further information available upon request.
[56] See http://uscountvotes.org/ucvAnalysis/US/election_officials/ElectionArchive_advice.pdf

Volusia County, FL. Council wise to reject Diebold bid, look for options.
http://www.news-journalonline.com/NewsJournalOnline/Opinion/Editorials/03OpOPN91061005.htm

Miami County beginning to see the expense and work of new DRE voting machines
http://www.daytondailynews.com/localnews/content/localnews/daily/0611elect.html

Florida: New concerns about electronic voting machines being hacked
http://www.tampabays10.com/news/news.aspx?storyid=14806

Florida - Diebold calls for investigation of Leon County voting machines
http://www.tallahassee.com/mld/tallahassee/news/breaking_news/11855543.htm

Volusia County FL's 'no' to touch-screens on state's radar http://www.orlandosentinel.com/news/orl-locvoting10061005jun10,0,4068868.story?coll=orl-news-headlines

Bibliography of Elections Papers Written by Kathy Dopp

Some Collaborative Papers written with PhD Statisticians and Computer Scientists:

Mar. 11, 2005 - Electronic Voting System Best Practices
http://uscountvotes.net/docs_other/dopp/Best_Practices_US.pdf

Oct. 20, 2004 - Summary: Utah Voting Equipment Selection Advice
http://utahcountvotes.org/voting_system_advice.pdf

July 1, 2004 - Suggestions for Writing an RFP for Voting Equipment
http://utahcountvotes.org/rfp_advice.pdf

Sep. 24, 2004 - Response to "American Attitudes about Electronic Voting"
http://utahcountvotes.org/Voting_systems.pdf

July 19, 2004 - Response to Request for Proposal for Utah's Voting Equipment
http://utahcountvotes.org/response.pdf

June 26, 2005 - Patterns of Exit Poll Discrepancies
http://uscountvotes.org/ucvAnalysis/US/exit-polls/USCV_exit_poll_analysis.pdf

Mar. 31, 2005 - Analysis of the 2004 Presidential Election Exit Poll Discrepancies
http://electionarchive.org/ucvAnalysis/US/Exit_Polls_2004_Edison-Mitofsky.pdf

June 29, 2005 - How Can Independent Paper Audits Detect & Correct Vote Miscounts
http://uscountvotes.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf

June 28, 2005 - What Election Data can Election Officials Collect and Publicly Release in Order to Monitor Election Accuracy?
http://uscountvotes.org/ucvAnalysis/US/election_officials/ElectionArchive_advice.pdf

August 18, 2004 - Concept for a Better Voting System
http://utahcountvotes.org/UVES_concept.pdf

This paper is publicly available on the Internet at
http://uscountvotes.net/docs_other/dopp/AdviceReDiebolds.pdf