What Could Be Worse Than a Hanging Chad?

It is no secret that elections have been influenced and possibly changed due to problems associated with electronic voting machines. One needs to look no further than the 2004 presidential election to find an instance where electronic voting methods resulted in many problems and malfunctions. In especially close races, one must question the accuracy of each vote counted. With electronic voting machines, we cannot always be sure that votes were accurately counted because there is not always a paper trail to show how the voter intended to vote. In fact, the integrity of electronic voting machines is a growing problem in the United States. In recent years, electronic voting machines have come under a great deal of scrutiny due to many discrepancies that have come to light. Despite the fact that electronic voting machines are easy to use, very efficient and supposedly thoroughly tested, the real problems with these machines result from the fact that there is no paper trail to provide proof of each vote, and that electronic voting machines are not nearly as secure from hacking and viruses as they need to be in order to ensure honesty and accuracy in the voting process.

In recent years, voters have seen shifts towards and then away from newer voting technologies due to the many problems resulting from these very machines. The 2000 presidential election was a huge turning point for the nation's voting procedures because of the "hanging chad" and "pregnant chad" phenomenon. Pregnant or hanging chads refer to the problem with punch-card ballots wherein the ballot is not completely punched, resulting in questions over voter intent. The inaccuracies with the 2000 elections in Florida caused an outcry for better voting technology. The issues raised in Florida involved punch-card ballots and other paper-based voting systems that were quickly deemed outdated and unreliable. Computers seemed like the best solution and the

government was intent on making "hanging chads" a thing of the past. Two short years after the mess in Florida, Congress passed the Help America Vote Act. This act was designed to improve voting systems in the United States. It authorized $3.9 billion in federal funds to replace old punch-card systems and lever machines with new electronic voting machines and optical scan machines (Pellerin, 2008, para. 13). However, many soon realized that the quick shift to electronic-based voting methods was one that would cause just as many, if not more, problems than the ancient paper-based methods had caused.

The elections in 2004 provided people with the reality check that electronic voting machines were no less immune to problems and controversy than their older counterparts had been. In the 2004 presidential election, a majority of the country used electronic-based voting methods. Estimates are that 35% of voters used optical scan machines, and 29.5% used electronic voting machines (Pellerin, 2008, para. 9-10). Optical scan machines are computer-based systems, but incorporate a paper trail that can be used as backup in case of problems. However, electronic voting machines are often paperless and there is no way to verify that votes were counted correctly. For example, in January 2004, a special election was held for a House seat in Florida. Paperless voting machines counted 134 ballots that were blank. It turns out that the race was decided by a mere 12 votes, but there was no printed record of the actual votes to show what the voters intended, and the results stood, regardless if they were correct or not (Batstone, 2004, para. 6). More problems associated specifically with the 2004 presidential election also began well before the election itself. In 2003, the CEO of Diebold Elections Systems wrote a letter to wealthy Republicans saying that he was "committed to helping Ohio deliver its electoral votes to the president." It just so happened that his company was bidding to supply electronic voting machines for the state of Ohio in the upcoming election (Batstone, 2004, para. 7). This conflict of interest

raised the question of how easily these machines could be rigged or hacked, and Diebold took a lot of heat after the elections in Ohio ended up being extremely close. The accuracy of electronic voting machines was questioned around the country because of problems, discrepancies, and flaws that were exposed during the 2004 election.

The years prior to and after 2004 were turbulent ones for electronic voting machines. Some argued that the software in electronic voting machines was vulnerable. They claimed that without proper testing and certification, electronic voting machines, also called digital recording electronic technology or DRE, could produce an incorrect report due to malfunction or deliberate manipulation (Schneier, 2004, para. 3). The use of electronic voting machines also brought about a political battle of some sorts. The Republican Party found itself closely linked to many CEOs and investors of companies that manufactured and supplied electronic voting machines. To more than a few Democrats, this situation raised the question of ethics and revealed a possible conflict of interest (Warner, 2003, para. 5). After the 2004 elections, many began to question whether DRE machines were the best method of voting. Electronic voting machines were supposed to be the saviors that provided a voting method that was completely computerized and eliminated all of the problems associated with old, paper-based voting methods. Instead, they brought about a new array of problems that seemed just as bad as, if not worse than, those associated with paper-based voting methods. It is no secret that no voting process will be completely safe from problems or flaws, but many began asking critical questions. Are electronic voting machines that much more reliable than paper-based voting procedures? Is the price of technologically advanced voting systems really worth the cost of questionable dependability?

The answer to these questions is a resounding no. In the case of electronic voting machines, the benefits do not outweigh the costs. There are simply too many problems associated with electronic voting machines to justify using such an unreliable and vulnerable method of voting. First, DRE technology has been found to be easy to hack. Second, electronic voting machines rely on computers, whose technology cannot be relied on to function properly. Computers are a very powerful resource; however, they can be manipulated and can cause enormous headaches when they do not function properly. In the case of electronic voting machines, those headaches come in the form of miscounted votes, subtracted votes, or votes left completely blank. Finally, another glaring flaw with electronic voting machines is the lack of a paper trail. All of the information is stored in computers and there are often no printed records to verify the vote. Some measures have been taken to resolve this problem. Currently, some states have passed laws that do require a paper trail with electronic voting machines. However, the federal government requires no such thing, and many states still have not adopted these controls (Zaldivar, 2006, para. 10). For these reasons, electronic voting machines cannot reliably be entrusted with counting votes in any election.

The proponents for electronic voting machines will argue many different points favoring the use of these machines. One argument favoring electronic voting machines is the fact that they are the most efficient method of voting. With DRE technology, all of the tallying is done by a computer and the days of counting votes by hand are gone. Perhaps this is a convenient aspect of electronic voting machines, but there are other voting methods that do not require counting by hand. Optical scan methods require the voters to fill out their choices in a box or oval, and then a computer takes the ballot and tabulates the vote (Pellerin, 2008, para. 9). This method is just as efficient as DREs, but there will always be the paper backup in case the computer malfunctions.

Some will also contend that electronic voting machines are a straightforward method of voting and speed up the voting process in general because they are simple and less confusing than other methods. However, these machines can be their own worst enemy. If one malfunctions or freezes up, the voting process can be made painstakingly long. For example, in 2006 in Colorado, new machines and a confusing ballot created long lines that forced people to wait over an hour to vote (Weisenmiller, 2006, para. 2). Those looking for an easy argument supporting electronic voting machines might suggest that these machines are easier to use than any other form of voting. Electronic voting machines require voters to touch a button on the computer screen. Sure, this might be the simplest method of voting, but does that really matter to voters? What voters really care about is whether their votes were counted properly or not.

Those in favor of electronic voting machines will also dispute opponents' claims that electronic voting machines are not safe from tampering or crashing. They contend that DRE machines are put through stringent testing and must pass strict guidelines before they can be put to use. In an article in the *Los Angeles Times,* the Executive Director of the Election Assistance Commission, Thomas R. Wilkey, explains this point. Wilkey claims that "federal guidelines call for extensive checking of electronic voting machines before delivery...states and localities usually perform their own testing too" (Zaldivar, 2006, para. 14).

However, Wilkey's claims are not exactly all that they are cracked up to be. Currently, the federal government does not enforce strict security and accountability standards for electronic voting machines (Zaldivar, 2006, para.10). Most guidelines and regulations are implemented at the state and local levels. In 2004, journalists from *The New York Times* went to Las Vegas to investigate how honestly and accurately casinos operate their electronic gaming machines. They

found that "protocols put in place on the Las Vegas Strip are much more stringent than those required for e-voting" (Batstone, 2004, para. 11). So people can be sure that they are losing their money honestly and accurately in Las Vegas, but they cannot be sure that their vote will be counted in a political election.

In addition, the testing done on the machines themselves is very secretive and confidential. Companies often will not make the testing results public and will claim trade-secret protection for their software. As David Jefferson, a computer scientist at Lawrence Livermore National Laboratory puts it quite accurately, "We are trying to run open, transparent elections on secret, corporate-owned software, and that to me is a fundamental contradiction" (Zaldivar, 2006, para. 16). That should be a fundamental contradiction for all voters in general. We cannot expect that all companies which manufacture electronic voting machines with the intention of making abundant profits will spend the necessary money to test their machines for security.

Finally, advocates of DRE machines contend that this method of voting is much more dependable than other paper-based voting methods. They argue that paper-based voting methods like punch cards and lever machines create many more problems than electronic voting machines do. They claim punch cards are difficult to use and when these cards are not used properly, the voter might cast a vote for the wrong candidate. They cite the 2000 election in Florida as a prime example of what is wrong with paper-based voting. A study done in the wake of the 2000 election found that up to 2 million votes were lost due to poor ballot designs (Boyle, 2004, para. 12). They also contend that paper ballots can be lost, changed, misread, or added to. However, these arguments fail to account for one thing. With paper-based voting methods, at least there is proof of how the voter actually intended to vote. There will always be a punch-card or paper ballot that

will provide at least some verification of how voters intended to cast their votes. With electronic voting machines, the vote is stored into the computer and lost forever unless a paper trail is required, which is no guarantee.

This lack of a paper backup is just one of the many reasons that electronic voting machines should not be used in any election. In some states, there are laws that require a paper trail or a receipt to confirm that electronic voting machines counted votes correctly. However, there are no federal laws requiring such thing, and even if a receipt is given to voters, can they be expected to verify and keep it? The lack of a paper trail also means that if the machine were intentionally programmed incorrectly, or even hacked, there would be no way to fully know the extent of damage done. The government can pass stricter regulations that require a paper-trail for electronic voting machines, but it cannot currently solve the other problems associated with electronic voting machines.

Furthermore, electronic voting machines cannot be trusted to tabulate votes accurately and fairly based on the premise that they rely on computers and computers are susceptible to viruses, software bugs, hacking, and crashes. There have been hundreds of instances in which the computers running electronic voting machines have malfunctioned and caused incorrect results. For example, in the 2002 Alabama general election, machines reversed the governor's race and 6,300 electronic votes mysteriously disappeared. A representative from Election Systems and Software, the maker of the machines, could only state, "something happened. I don't have enough intelligence to say exactly what" (Harris, 2003, 11). In addition, in dozens of those elections, the computer named the incorrect winner. In a 2002 election over a school bond issue in Nebraska,

electronic voting machines failed to tally "yes" votes and incorrectly declared that the measure had failed miserably. However, the measure actually passed by a two-to-one margin (Harris, 2003, 12).

Electronic voting machines are also unreliable because they are susceptible to tampering and hacking. Harmful software could be installed on a machine without being noticed. In 2003, Avi Rubin, a professor of computer science at Johns Hopkins University, and Dan Wallach, a professor at Rice University, performed an analysis of a DRE machine and found that the software was vulnerable to hacking and manipulation (Pellerin, 2008, para. 14). On top of this study, in 2006, a Princeton University computer scientist and graduate students tested a Diebold AccuVote TS voting machine. They found a way to hack into the machine's computer software and changed votes from one candidate to another, without leaving a trace (Weisenmiller, 2006, para. 16).

In conclusion, electronic voting machines were rushed into elections far too quickly and were left with many flaws. They were supposed to bring about a new era of voting technology. Nevertheless, they simply became another voting disappointment after accounts of setbacks and flaws began to escalate. From the beginning, they had no paper trail to verify votes and questionable partisan ties. Even after all the scrutiny regarding the lack of a paper backup, the federal government has not taken measures to require that all electronic voting machines have a paper trail. As DRE technology began to be used more frequently, accounts of errors and breakdowns accumulated. Now it is time to end the use of electronic voting machines in favor of more reliable methods that include an automatic paper trail. We should not be sacrificing the integrity of voting to achieve speed and efficiency.

References

Alonso-Zaldivar, R. (2006, November 3). E-voting may be scarier than hanging chads; computer bugs, paper backups, hackers -- some fear electronic balloting will be a whole new headache. *Los Angeles Times,* p. A18.

Ardizzone, S., Michaels, R., & Cohen, R.C. (2007). *Hacking democracy.* [Video/DVD] New York, N.Y.: Docurama: New Video Group.

Batstone, D. (2004). The machine ate my vote. *Sojourners Magazine, 33*(9), 19.

Boyle, A. (2004). Sparks fly in e-voting debate researchers face off over security issues. Retrieved October 14, 2008, from http://www.msnbc.msn.com/id/4274389/

Card, D. E. (2005). *Does voting technology affect election outcomes?: Touch screen voting and the 2004 presidential election.* Cambridge, MA: National Bureau of Economic Research.

Duschere, K & Lopez, P. (2008, November 11). Coleman leads Franken by 206 votes. *Star Tribune,* p.1.

Harris, B. (2003). *Black box voting: Ballot tampering in the 21st century.* High Point, NC: Plan Nine Publishing.

Pellerin, C. (2008). *Debate continues over security, reliability of voting technology: Many states, localities may turn to paper ballots for November 4 elections.* Retrieved October 13, 2008, from http://www.america.gov/st/elections08-english/2008/August/20080827151002lcnirellep2.584475e-02.html

Rice University; hack-a-vote: Students at Rice learn how vulnerable electronic voting really is. (2008, October 23). *Computer Business Week,* 137.

Shneier, B. (2004). *The problem with electronic voting machines.* Retrieved November 12, 2008, from http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html

Warner, M. (2003, November 9). Machine politics in the digital age. *New York Times,* pp. 1-3. Retrieved November 12, 2008 from, http://www.nytimes.com/2003/11/09/business/machine-politics-in-the-digital-age.html?n=Top/Reference/Times%20Topics/People/W/Warner, %20Melanie

Weisenmiller, M. (2006). U.S. elections: E-voting squeaks by with a few glitches. *Global Information Network,* 1.

Weiss, T. R. (2008). Proponents, critics give no ground in tussle over E-voting. *Computerworld, 42*(21), 12.