

15

Privacy Implications of Voting Technologies

Graham Eno and Meghan McCormick

Introduction

Regardless of political party affiliation, reflecting on the problems that occurred in Florida's 2000 presidential election can make anyone uneasy considering we all have a stake in the successful execution of the democratic process. A repeat of the spectacle in Florida is not in anyone's best interests, and therefore, must be avoided at all costs. Yet, four years have passed and it seems that we are not any closer to having developed a solidified and accurate voting system to use in the 2004 presidential election and in the election years to come. This is not to say that successful elections utilizing either older punch-card machines or machines recently developed that use touch screen technology have not been held in other countries. The challenge however, arises when it becomes necessary to measure an enormous popular vote, as in the United States. As we have seen in past presidential elections, emotions seem to run as high as the security threats.

Florida 2000

In order to obtain a greater understanding of the situation that needs to be avoided in any election, let's recap what happened in Florida during November 2000. Certainly, many factors played into the discrepancies, delays, and controversy surrounding Florida during the 2000 presidential election. Among them include the "disenfranchisement" of African American voters. A majority of African American voters who, traditionally, vote democratic were "cleansed" from the voting register for felonies that many of them never committed. A civil rights panel in Florida issued a report blaming the corruption on Florida Governor Jeb Bush, his brother George W. Bush,

and the former Floridian Secretary of State Katherine Harris. The panel concluded that:

Black voters in Florida were disproportionately the victims of faulty voting equipment, erroneous registration rolls, overwhelmed phones at county election headquarters, last-minute polling-place switches and potentially intimidating police presence at heavily African American precincts (Calmes 2001, p. A.24).

In the end, “an estimated four million to six million ballots [nationwide] were not counted or were prevented from being cast at all” (Selker 2004, p. 92). This is not just an unethical scenario; it is completely illegal and discriminatory. Furthermore, given the narrow margin by which Bush won, it could have changed the overall outcome of the election. All other factors aside, what exactly was it about the faulty voting equipment that made it so difficult for each and every citizen of those respective counties in Florida to cast their vote accurately and have it counted truthfully?

Ballots and Methods

The balloting methods used in Florida did not differ drastically from those used around the rest of the country during the 2000 presidential election. However, it was the epicenter of balloting confusion at that time. For a moment, let us look at how voting methods have developed into a need for more sophisticated polling methods in America.

As with most areas of technology, methods of casting a vote have changed drastically over the years. The use of a ballot, which is defined as “a sheet of paper or a card used to cast or register a vote, especially a secret one to choose a particular candidate” dates back to 139 B.C. (dictionary.com and glencoe.com 2004). Hand-counted paper ballots are still used in 1.3 % of America today; however, most states have upgraded their methodology (Selker 2004, p. 94). The first technological advancement in voting machines came with the mechanical lever. To use a lever voting machine, one would enter the bulky machine and pull the lever of the candidate for whom one wished to vote. Lever machines were used throughout the fifties up until the 1996 presidential election (glencoe.com 2004). Punch card machines slowly began to replace lever machines in the 1960's. This method allows the voter to use a stylus to punch through a perforated hole next to the candidate of their choice. When the voter punches through the card, the perforated circle that detaches is referred to as a “chad”. This is the notorious balloting system that was implemented in many of the counties in Florida in which, during the recount, the “hanging chad” epidemic arose. That is, the card had more than one chad hanging from it due to weak perforation on the remaining chads. Those performing the manual recount could not determine which selection the voter had originally made. This method was an improvement upon the last two methods, but clearly, a much more reliable system needs to be developed.

Internet Voting

To eliminate error and speed up the voting process, many states around the U.S. are looking toward Internet voting. With the popularity of the Internet today, it is tempting to develop a voting system online. Voters could cast their ballot from the convenience of their home computer. Internet voting sounds great until one considers how dangerous putting a vote on the Internet is. Not all the dangers existing around Internet voting are strictly related to viruses. Hackers could manipulate the vote by cracking source code and increasing the vote count for one particular candidate. This could potentially breach voters' privacy by exposing the voter registry as well as an individual voter's selection. In January of this past year, Deputy Defense Secretary Paul Wolfowitz proposed a system to have military personnel stationed domestically and overseas, vote utilizing an Internet voting system. A commission reviewing the proposal determined the administration was getting ahead of itself, not considering the insecurities of the Internet and the lack of any guarantee against manipulation or fraud. Four years ago, overseas military ballots also contributed to the controversy surrounding the 2000 presidential election's outcome. Ballots received after the cut-off date or that did not have a postmark on them were immediately thrown out. With more men and women in the military and in the civilian sector of the military service industries deployed overseas since the Vietnam War, their votes could significantly sway the 2004 election and those in the future. Therefore, it is imperative that we are able to develop a system that allows those sacrificing so much for this country to have their voices heard. Though Internet voting does not appear to be a current option, the implementation of localized electronic voting machines has been executed, and done so successfully in many states and even in other countries such as India.

DRE Machines

So what exactly is an electronic voting machine? Electronic voting machines are specifically referred to as direct recording electronic systems, which we will refer to as DREs from here on out. DREs usually consist of either a touch-screen computer or a computer screen with buttons along the sides of the screen for vote selection (similar to an Automated Teller Machine). Typically, a keyboard is provided for write-in candidates who do not already appear on the screen. Once a voter makes their selection, a button is pushed to cast their ballot and a friendly message pops up on the screen stating their vote has been cast and thanks them for voting (Diebold 2004). The main problem with these machines is that there is no paper trail produced to verify votes. All votes are stored on the machine's hard drive. At the end of the voting day, officials simply look up the total tallies for each candidate on each machine and determine a winner (Diebold 2004). This sounds easy enough but what if the system crashed, or hackers were able to penetrate the system and change the votes? This would destroy the data's integrity resulting in a questionable election outcome. Some competitors in the DRE industry are trying very hard to solve this problem.

VoteHere, a company that adds paper trail capabilities to existing DREs, has developed a system where the voter has the option to print

two different types of receipts. The first would confirm that one voted and would have a unique identifier so election officials may trace the ballot number back to the selections that was made at the poll. The second form would be a detailed receipt that allows the voter to enter an alphanumeric pass code that is private to them. It will appear next to the selections that they made when voting (votehere.com 2004). In order to ensure the voter's privacy, every possible choice is printed on the receipt with randomly generated numbers next to the selections that the voter did not choose. The voter's privately selected code appears next to the candidates the voter chose so only the voter can later identify their choices on the receipt. VoteHere is also the first company to release the source code to its machine so it can be publicly scrutinized. In a sense, VoteHere is almost turning the task of securing their electronic voting systems into an open source effort, which could have both positive and negative implications regarding the security of the code (votehere.com 2004). Recently, the source code for one of Diebold's most popular model of DRE was inadvertently placed on the Internet. When the code was discovered, a John Hopkins computer science professor by the name of Aviel Rubin and a group of computer security experts analyzed the code upon downloading it. They proceeded to produce a report that told of the many flaws in the code. Rubin told *Wired Magazine* "they made mistakes I wouldn't expect an undergraduate in computer security to make" (Frankel et al. 2004). These are very real threats that only scratch the surface of ethical issues that must be addressed before these machines are used nationwide.

PAPA

The problems regarding DREs align almost perfectly with the four Information Technology ethics categories founded by Richard Mason, whose work has been the ethical standard in the industry for almost 20 years (Brobst and Hackathorn 2004, p. 53). The first of these categories is privacy, which is fundamentally applicable to the electronic voting process. The utilization of a secretive balloting method has been a universal practice thought to be essential for a free society to operate (Coney 2004). In today's passionate political climate, a voter should arrive at the polls with the utmost confidence that he or she can cast their vote free of ridicule or harassment and ultimately based on their own personal values and beliefs. The moment this right is withdrawn, our democracy will crumble.

The second category Mason dictates is that of accuracy, in terms of data quality and liability. The DREs do not have a concrete system of verifiability. A paper trail is needed to account for each and ensure every vote was cast accurately. The moment something adverse happens to the machines or the network, a recount must be taken, and that cannot happen without some form of physical record.

Third, in terms of electronic voting, we must ask who it is that claims ownership of these machines. Mason phrases this as property. The answer to this question may seem obvious in that the government owns them. However, ownership of a source code differs from that of a physical machine. The true owners of the machines are the companies who built them, wrote their source code, and guaranteed their security and reliability. The blame and reliability for a voting mishap stops with

them. Furthermore, once the last vote is cast, it is the responsibility of those totaling the votes and extracting the data from the machines to maintain and ensure its integrity.

The final category proposed by Mason is accessibility. Accessibility relates to electronic voting in two ways. First, who can access a vote cast on an electronic voting machine. Imagine the extreme misrepresentation of the country's popular vote that could occur if hackers penetrated the system and were able to change votes. The frightening reality is that the machines currently in use do not have the proper security features installed to protect the votes cast within them. On the website 'blackboxvoting.org,' they show a monkey who by pushing buttons on the keyboard was able to erase all ballots that had been cast on a Diebold voting machine.

Another form of access that affects DREs is usability. For instance, in the past, voting was problematic for disabled voters. They lost the right to cast a private vote and had to rely on the assistance of others. Bi-partisan representatives as well as an election commission representative would have to be present in order for them to vote. Now, many DREs are "equipped with technology that allows the disabled to vote independently" (2004 cnn.com). For the first time in the U.S., disabled voters can cast a private ballot.

In addition to assisting disabled voters, the new electronic voting machines are much more user friendly than the machines of the past. Part of the confusion in Florida was a direct result of how confusing and unclear the ballots were. Electronic voting machines guide the voter through the voting process as well as give them an opportunity to confirm their candidate choices before casting their ballot, making them systematically easier to use. However, the security flaws inherent in the current machines allows for plenty of speculation as to their accuracy, honesty and ability to precisely represent the will of the American people in an election environment.

Finally, DRE voting will also make voting easier for voters whose first language is not English. DRE machines can be programmed to offer a screen in many languages. This would allow a voter to choose a language to guide them through the voting process. After the voter has made their selection, DREs with printing capabilities could print the ballot in English regardless of what language the voter made their selection in. Considering that 31.8 million Americans speak a language other than English, this feature puts DREs strides above other voting technologies. (ethnicharvest.org 2004).

The Path to DREs

So far we have revealed both pros and cons of voting technologies in the U.S. today. From hand-written ballots to DREs, voting methods in this country are rapidly changing. Calls for an improvement of voting technology was heard loud and clear after Florida 2000, which led to the enactment of the Help Americans Vote Act (HAVA) of 2002. With a multi-billion dollar budget, this act is helping to fund DRE implementation nationwide; yet, we have also shown how this money has fueled bad business practices, and how HAVA seems to be falling short of its goals. In addition, we argue that HAVA has nearly ignored the issue of privacy within the voting process, and has yet to tackle the

issue of paperless DREs. Issues concerning developing a paper trail and regarding voter security are being left at the state level instead of forming a uniform method for nationwide use. Furthermore, a nationwide method of voting that employs a traceable paper trail will result in a higher level of voter and candidate confidence. If the United States is ever going to wean itself off of the Electoral College, and allow every popular vote to determine the presidency, there needs to be a uniform voting system nationwide. We conclude with an overview of early results of the 2004 election. For the first time, portions of the nation voted using DREs. In the end, it appears that the 2004 election went smoother than 2000, and we can only hope that if HAVA does all it is suppose to do, the 2008 election will be the most uneventful, accurate presidential election to date.

DRE Manufacturer Corruption

In order to insure there will not be any conflict of interest between companies producing DREs and people voting on them, we have to analyze some of the major players in the industry. Diebold Election Systems, based in Ohio, is by far the largest manufacturer of these electronic machines. However, the company is a strong Republican contributor and their "CEO Waldon O'Dell promised in a fundraising letter to deliver Ohio's electoral votes to President George W. Bush" (Frankel et al. 2004, p. 5). This caused a public outcry and after further investigation, it was discovered that O'Dell was a "pioneer" in the President's fundraising hierarchy (electiononline.com 2004). In fact, between 2001 and 2004, Diebold has contributed over \$400,000 to Republicans and just \$2500 to Democrats (electiononline.com 2004). It is obvious where their loyalties lie. Since the realization of this serious skew in personal interest, the executives at Diebold have established a policy eliminating the contribution of any money to either party in order to avoid just this kind of press and public outcry. However, when looking at the financial contributions being made by other DRE manufacturers, the overall playing field is fairly level with essentially no significant difference in the amounts given to each party's efforts. Election Systems and Software, which is based out of Nebraska, gave \$24,550 to democrats and just under \$22,000 to republicans (electiononline.com 2004). Problems do arise when looking at where some election officials and even candidates used to be employed. The public has come across its fair share of candidates and officials that had once held executive positions in these companies causing one to speculate over the honesty of their machines' results.

If the skewed campaign donations are not reason enough to believe that Diebold has a severe conflict of interest, consider this:

"Diebold makes a lot of ATM machines. They make machines that sell tickets for trains and subways. They make store checkout scanners, including self-service scanners. They make machines that allow access to buildings for people with magnetic cards. They make machines that use magnetic cards for payment in closed systems like university dining rooms. All of these machines that involve data input that result in a transaction, just like a voting machine. But unlike a voting machine, every one of these other kinds of Diebold machines -- *every one* -- creates a paper trail and can be audited. ... These machines [all] affect the

livelihood of their owners. If they can't be audited, they can't be trusted. If they can't be trusted, they won't be used" (Cringley 2004).

In true economic fashion, if Diebold machines "can't be used" then Diebold wouldn't have a customer or a profit (Cringley 2004). So the question remains, what provoked Diebold to omit a paper trail with their voting machine product? The unanswerable question is, did Diebold choose to make their product not auditable, or were there outside forces at work here (Cringley 2004)? Diebold's refusal and uncooperative manner regarding the implementation of a paper trail on their DREs, is highly unethical and raises questions as to their reasons for doing so.

HAVA

In America, voting is considered both a right and a responsibility. It is a private, personal act within a large, complex and highly visible system. At its best, the system generates public trust and confidence in the electoral process and legitimizes the outcomes; at its worst, it fuels cynicism, distrust, and, in the extreme, efforts to overturn the election (Frankel et al. 2004, p. 1).

The disaster of the Florida 2000 election, discussed earlier, fueled a reform of the voting process in the U.S. Specifically, it provoked the development of the Help America Vote Act (HAVA, Public Law 107-252) (Frankel et al. 2004, p. 7). This act was developed to help states upgrade all of their voting machines to DREs by 2006. \$3.9 billion dollars were allocated to the effort, and naturally, many companies jumped at the opportunity of being the DRE provider-of-choice. In fact, Diebold, the current leading manufacturer of these machines was so eager to jump on the \$3.9 billion dollar band-wagon, that they "[bought] a smaller company that made voting machines just to get into the market" (Cringley 2004). Yet in the rush to sell their product, they neglected to add paper trail making abilities to the machines. With an ever-advancing deadline for states to switch all of their voting machines to DREs, it is critical that these machines are well chosen, and states are conscious of the traditional DREs' lack of a paper trail. After all, the outcome of every election in the future will depend on these machines.

"The Caltech-MIT Voting Technology Project, a study group set up to analyze elections dating back to 1988, found that old-fashioned lever machines were actually more accurate than electronic voting machines" (Lougren 2004). This is cause for concern, considering one-third of American voters used a DRE in the 2004 election, up from only 10 % of voters in the 2000 presidential election (Lougren 2004). These inaccuracies make us question whether this is a technological problem or the result of a familiar company's agenda. Until 2006, every state mandates the rate of their switch from current voting machines to DREs. This "de-centralized" system has led to many different methods of DRE implementation and rate around the nation (Frankel et al. 2004, p. 9). In Ohio, for example, the state that determined the 2004 presidential election, "72 % of registered voters – more than 5 million people – will be using punch cards to vote" (Frankel et al. 2004, p. 9). Ohio was hesitant to switch machines for the 2004 elections when

“consultants found serious security flaws in the DRE technology offered by four of the nation’s top vendors, and decided to delay deployment of electronic voting systems” (Frankel et al. 2004, p. 9). Though HAVA was employed with good intent, there must be a serious look into the security risks elections will be faced if they use paperless DREs.

Privacy

According to new requirements that have been established by the Federal Election Commission, the newly developed DRE voting machines must, at the very least, record each vote without exposing any information about how an individual voted. This is required before any certification is given to any of the different DRE machine designs. This, nevertheless, is not enough. Anonymity is not the only requirement of the DRE with respect for privacy, but in fact each time a vote is cast it is assigned a time stamp. If someone were able to get their hands on this related information they could distinguish a great deal about an individual, diminishing anonymity. Enough information could be compiled from the date/time stamp, the party that the affiliated ballot supported, and camera footage from many different types of cameras watching the polling place, a correlation of vote to voter could be made (Frankel et al. 2004, p. 10). Much of the time, the way a voter’s identity and the way they cast their vote creates confusion at a precinct and the voter must disclose who they are in order to authenticate their ballot, their vote, and most of all their voting eligibility. As a matter of fact, anyone could go on the Internet to a precinct assignment website and using nothing more than a person’s last name and a matching birth date, can access address information, phone numbers, and even party affiliation.

The way that the new DREs are designed, the voter is forced to use some sort of key, whether it be a PIN code, a password or a smartcard in order to access the system and actually cast their vote. Similarly, in elections abroad, countries mark a voter’s hand using permanent ink or a stamp so that repeat voting is prevented. Assuming that there is an effective paper trail produced by the machines, the DRE itself will maintain a record of votes on its memory cards. However, the voter themselves should be able to take the paper receipt produced by the DRE and review it, confirming their selections and then casting that into another secure ballot box where it is supposed to be kept safely by election officials in the event a recount is needed. The problem with using these smartcards is that the voter’s identity is indirectly contained on the card. The voter’s smartcard contains their voter registration number. This alone is not a problem; however some companies, such as Diebold, handle voter registration database management tasks, which could be compared with the numbers contained in the smartcard, revealing the way the voter cast their ballot.

As we have established before, casting a ballot in privacy is critical in the democratic system of voting, and is difficult to obtain with DREs. The problem lies between “anonymity vs. audit ability” (epic.org 2004). In short, in order to verify a vote, it must be traceable. Nevertheless, this jeopardizes the right to cast a private ballot. Moreover, in order “to make voting results anonymous, these machines [DREs] randomize the voting sequence, which also makes it impossible to trace their accuracy”

(epic.org 2004). Here, instead of having the machine randomize the votes, the power needs to be in the hands of the election officials. As is seen in Vote Here's VHTi system, election officials are able to "create the keys that will be used to shuffle and decrypt the ballots after the election," while maintaining the anonymity of individual voters (votehere.com). This is a step in the right direction of what needs to be a main concern with DRE development in the future. At no other time in American history has the outcome of an election been so dependent on the manufacturers of the voting machines. Current DREs force election officials to place utmost trust in the manufacturer's word that their machine will produce an accurate vote count. The key is to "remove reliance on the vendor of the electronic machine from the process" (Rubin 2004, p. 2). For as Jim Alder, founder of VoteHere, Inc. put so well, "there is no security in obscurity" (2004 Alder, p. 4). Votes must be printed out on an individual basis, not hidden within the depths of a DREs hard drive.

DREs of the Future

This automatically poses the next question; does strict reliance on a hard-drive even belong within the voting process? Is there a way to keep all the benefits of current DREs while switching away from data storage and instead towards data production in the form of an auditable paper trail? Many want to abandon DREs completely and go back to a purely paper system, yet, we argue that is not the solution nor is it possible considering the millions of dollars states have already invested in DREs around the nation. Time has shown, as technology grows, society naturally grows along with it. There is a place for DREs in the U.S.'s election system, with a few improvements of course.

Realizing the risk of sounding too bold, if we were to build a fool-proof DRE to be used in elections after 2006, we would need to make quite a few additions to the machines currently on the market. First and foremost, they would print out a paper trail for an accurate audit, and a receipt for voter-verification. Instead of storing votes on a hard-drive and printing out a grand total at the end of the Election Day, machines would printout each ballot, which could be confirmed by both the voter and election officials. This would also provide a solid means for a recount if needed. In addition to the ballot print-out, the machines would print out a voter-verification receipt. In short, a voter could assign their own private "key" to their vote for each candidate, which would be printed out on a receipt for them to take home. For instance, let's say they were to assign the key ABC to their Presidential choice. The machine would print-out a receipt with the key ABC under the Presidential category along with different assigned keys under every other category they voted on. This allows the voter to verify that their individual vote was counted without sacrificing their private, identifying information such as their name or social security number. After the votes have been counted, a voter can look on a publicly posted election results list for their specific key to show that their individual vote was counted. This technology is currently being employed by VoteHere, Inc., a company that adds paper printing capabilities to current paperless DREs (votehere.com 2004).

Standards

In addition to allowing voters to verify their own vote with a voter verification receipt, making the public aware of testing and certifying methods used can help increase voter trust of DREs. As another part of HAVA, the National Institute of Standards and Technology (NIST) has been given the responsibility of developing “standards for machine accuracy and security of the software and hardware to be implemented by 2006” (Frankel et al., 2004 p. 19). Even though the NIST has been aware of their role since the inception of HAVA in 2002, very little has yet to be accomplished in accordance to developing standards for DREs. One reason this may be occurring is, as of now, a majority of decisions about DRE implementation is made on the state level. So far, according to the NIST website, they have studied issues concerning screen layout and worked with the American Foundation for the Blind to determine the best format for handicapped voters (nist.gov 2004). The NIST website states that a main goal of theirs is to, “ensure that there are standards and testing methodologies that provide people with the means to cast a valid vote quickly and independently, and feel confident that it was cast as intended” as well as find a way “that allows poll workers to set up the machines properly and easily” (nist.gov 2004). To date, NIST has exhausted all funding made available through HAVA, and has had to pull money out of other areas of its budget to supplement the project (nist.gov 2004). The lack of funding has severely slowed the process, most tragically affecting the development of guidelines for installing ballot-printing functions onto existing machines. They are requiring that every state have an auditable paper trail on all their machines by 2006, but there is no regulation or standards set up to accomplish this so far. Right now it is up to individual states to decide how the paper trail will be produced on their DREs. This is a critical step considering statistics show that 77% of Americans would support DREs if they had a paper trail compared to 53% without (“As Election...”). Furthermore, 69% of Americans believe DREs need a paper trail “even if [it] adds significant cost to conducting elections” (“As Election...”). Setting standards and guidelines for states to follow in their implementation of the DRE switch over was one way to help the public feel more secure about DRE voting systems. Clearly, the NIST has not come close to doing this in the past four years and as it appears, is unlikely to do so in the future.

Election 2004

The presidential election of 2004 is one that is thought by many to be the most important of our lifetimes. Voter registration skyrocketed, and both parties expected an extreme increase in voter turnout at the polls. This, in combination with all the new DRE machines, causes some to speculate as to whether the machines would be able to actually handle the sheer numbers that would be using them. Many states employed a method for dedicated voters to actually cast their vote at designated polling places up to a week before the election. In turn, this early voting has been viewed as the main reason that disaster did not occur on November 2, 2004. Even though turnout at the polls had voters waiting for up to 4 hours in line, a majority of the machines held it together, and it is thought by many election officials that this election

was significantly more accurate than its predecessor in 2000. This does not mean that the election went off without a glitch, considering that over 120 million people came out to their precincts, turned in absentee ballots, or cast a provisional ballot. This number was only to be exceeded in the 1960's, during the Vietnam War.

In Florida, problems arose almost immediately as polls opened, but not on the widespread scale that was to be expected. About ten DRE machines failed in Broward County. Of course there were also the usual registration discrepancies that ultimately caused people to go from one polling place to another in order to accurately and legally cast their vote (2004 abclocal.go.com). In addition, this election was monitored by an incredibly large number of watchdog groups and lawyers. The number of lawyers employed by both parties was running upwards of 20,000 by November 2, 2004. That many lawyers can mean only one thing, that many egos. Many thought that this would end up being an incredible disaster, however, only a small number of lawsuits were filed when compared to the larger possibility of conflict. On top of the legal representation present by both parties, there were a large number of independent groups established to help voters who had equipment trouble, felt pressured, intimidated or harassed, and even to help those who felt they should be properly registered at a specific precinct. One such group is VerifiedVoting.org which has tracked almost all the cases in which machines were not properly emitting a paper trail (verifiedvoting.org 2004). They also pioneered the fight to demand that we had a paper trail on a majority of the DREs used in this election. Their efforts paid off even though a true statewide or nationwide recount was never requested (2004 verifiedvoting.org). Many people believed that Election 2004 was going to be a complete debauchery but instead it came and went just as an election should. The only delay in the outcome was in states where the results were so close the states were designated "too close to call" by many of the television networks reporting the results. Officials nationwide are breathing a sigh of relief that this election played out much like the Y2K paranoia, without much incident.

It is clear that voting methods need to be reformed in the United States. DREs are going to be fully integrated into the voting system. Yet, we believe we have shown that this installation of DREs must happen under strict guidelines. Security and voter privacy are two main concerns that could, if not handled properly, jeopardize elections in the future. Overall, DREs and other technological advancements concerning voting are needed, nonetheless, executing this will be a risky endeavor.

Works Cited

- "As Election Day Approaches, New Poll by WPI Shows Americans Have Concerns About Electronic Voting Machines." Worcester, Mass., 21 October 2004. *Black Box Voting Website*. <www.blackboxvoting.org> 3 October 2004
- Adler, Jim. "Electronic Voting Machines." Capitol Hill Hearing Testimony. 20 July 2004. <http://web.lexisnexis.com/universe/document?_m=2b95fc7423b12839620434ab21d4aae4html>.

Brobst, Stephen, Richard Hackathorn. "The Future: eXtreme data warehousing." *Teradata Magazine*. 2004. <teradatamagazine.com>

Calmes, Jackie. "Rights Report on 2000 Vote Fuels Debate Clouded by Ambiguities." *The Wall Street Journal*. 11 June 2001. A.24.

Coney, Lillie. "Hearing on Human Factors and Privacy". *The Electronic Privacy Information Center*. 2004. <http://www.epic.org/privacy/voting/voting_statement.pdf>

Cringely, Robert X. "No Confidence Vote: Why the Current Touch Screen Voting Fiasco Was Pretty Much Inevitable." *PBS Online*. 1 November 2004. <<http://www.pbs.org/cringely/pulpit/pulpit20031204.html>>.

Dictionary.com Website. <www.dictionary.com> 3 October 2004.

Diebold Company Website. <<http://www.diebold.com/dieboldes>>. 3 October 2004.

"Disabled Hail E-Voting Despite Doubts." <<http://www.cnn.com/2004/TECH/Internet/10/04/better.e.voting.ap/index.html>> 3 October 2004.

Election Online. 2 November 2004. <<http://www.electiononline.com>>.

Electronic Privacy Information Center Website. 31 October 2004. <<http://www.epic.org/privacy/voting/>>.

Ethnic Harvest Website. 2 November 2004. <<http://www.ethnicarvest.org/regions/50languages.html>>

Frankel Mark S., Tova Jacobovits and Adrienne Kroepsch. "Making Each Vote Count." *A Research Agenda for Electronic Voting*. October 2004. American Association for the Advancement of Science <http://www.aaas.org/election/Electronic_Voting_Report.pdf>.

"History of Voting Machines." Glencoe textbook online supplement. Electronic. Glencoe. <http://www.glencoe.com/sec/socialstudies/btt/election_day/history.shtml>.

Lougren, Stefan. "Are Electronic Voting Machines Reliable?" 1 November 2004. *National Geographic Online*. 2 November 2004 <http://news.nationalgeographic.com/news/2004/11/1101_041101_election_voting.html#main>.

News 13 in Toledo Ohio Online. 1 November 2004. <http://abclocal.com/wtvg/news/1102_florida.html>.

NIST Website. 1 November 2004. <<http://www.NIST.gov>>.

Rubin, Avi, Dr.. Interview. *Talk of the Nation*. National Public Radio. 14 May 2004.

2004 Selker, p., Ted. "Fixing the Vote." *Scientific American* 291.4 (2004): 90-98.

Verified Voting Website. 1 November 2004. <www.verifiedvoting.org>.

VoteHere, Inc. 1 November 2004. <<http://votehere.com>>.