

## Electronic Voting

The right to vote is considered almost sacred in the United States of America. Many groups have struggled to win that right and it is the backbone of democracy. While voting may seem to be a straightforward process, the task of choosing a satisfactory system to conduct a vote has proven to be a daunting one and many problems have arisen. Several techniques have been devised to solve them, but each presents unique roadblocks. Electronic voting is the latest of these attempted solutions and it comes hand in hand with the Information Age, addressing many of the difficulties presented by physical voting methods. However, along with the problems it attempts to solve, it inherits many of its own from the age in which it comes. In order to fully understand electronic voting and to evaluate the characteristics it needs to have, we must consider the interests of all the parties involved. Thereafter, discussing the advantages and disadvantages of the solutions currently proposed will allow us to reach a definitive conclusion about the viability of an electronic voting system.

As Karl Stephan notes, there are many individuals and groups of people in the United States that are interested and invested in the outcome of an election. Most states have different voting requirements, and anyone that meets them has a legal right to vote. The candidates are also involved in the election and have a right to expect a reasonably accurate tabulation. However, they do not have a right to a perfect count, because that would mean that the detection of one flaw would throw out an entire election. In addition to these two groups of people, the election officials, vendors of voting systems, and engineers of the systems all have a vested interest in the outcome of the vote. Therefore, it is necessary to create a system that meets the standards of all of these groups (Stephan).

Bruce Schneier, a technology security expert, believes it is necessary to consider four required characteristics that a successful voting system must have. These are accuracy, anonymity, scalability and speed. Accuracy is a very important factor when it comes to voting because of the great importance of the decision. The system should capture the intent of the voter and translate that directly into a counted tally. In order to have an accurate vote, the system must be secure. In a secure system, it should not be possible to change a person's vote or in any way affect the accuracy of the outcome. In addition to accuracy, anonymity is the driving force behind an effective voting system. A successful system will need to implement anonymity to the highest degree. Scalability is also a very important factor. A vast number of people around the world participate in voting in their own countries. In the United States, more than one hundred million people vote for President. A large number of people in India and Brazil vote in their own elections, with 372 million and 115 million voters, respectively (Schneier). Therefore, it is of the utmost importance that the system be very scalable and hold up against the massive number of incoming votes. Elections are also frequently very complex; many different elections are taking place the same day in different parts of a country, and the system should be able to support this. Speed is a very important aspect as well, as people in the United States in particular expect the votes to be counted and finalized before the day of the vote is over. A system will need to provide results extremely quickly while maintaining accuracy.

Over the years, there have been many attempts to perfect the voting process. Five main types of voting systems have been used in the United States. These include paper ballots, punch-card machines, optically scanned ballots, mechanical lever machines, and direct-

recording electronic (DRE) voting machines (Mercuri). Paper ballots were the leading medium for voting twenty years ago, but have since been replaced by other methods. Paper ballots are usually completed using a pencil and are manually counted to tabulate the results. For recounting purposes, the original is always available. Punch cards use a metal punch mechanism to record choices and cards are counted by a computer. Similar to paper ballots, each original card is available after the automatic count. In the case of optically scanned ballots, each one has a circle to darken or an arrow to complete by the voter to indicate his or her choice. The ticket is then optically scanned and counted by a machine. Like paper and punch-cards, the original is left as evidence. Mechanical lever machines use switches to indicate each candidate or option, and a machine keeps a running count of the tally. The subtotals remain on the machine, but there is no physical evidence of the results (Mercuri).

The most technologically advanced systems in use today are called direct-recording electronic devices or DREs. A DRE is very similar to a personal computer and uses a display to let the user see the voting options. Each option can be activated by the voter, usually via buttons or a touch screen. A keyboard is usually provided to support write-in votes. The choice is then stored locally in the machine's memory. After the election, the results are tabulated and added to the results of other forms of voting. Sometimes the votes are printed in order to provide an alternative hand-counting method. The tally from one machine is added to others in order to create a full count. While there is no physical evidence of the tallies, they are collected and stored on the hard disk of the computer ("Electronic Voting"). In 1980, 75% of United States counties were voting on either paper ballots or mechanical lever machines. By contrast, in 2000 less than one-third used the same methods. Instead, more counties were now using the

optically scanned ballots than any other type, with a 40.2% share of the votes. DREs were also becoming more popular, tabulating 8.9% of the votes cast. Punch-card machines were still quite popular, with usage rates of 19.2%, but it is believed that this number will drop off significantly in the future because of inherent problems with the system (Mercuri). In 2004, it was shown that 675 counties in the United States, which amounts to 30% of all registered voters, used some kind of electronic service to vote in the elections (Lin and Espinoza).

Physical voting and electronic voting each carry inherent advantages and disadvantages which are important to consider in forming an ethical conclusion about either method. While it would be nearly impossible to consider every advantage and disadvantage, it is necessary to evaluate at least the most important ones. Paper voting carries many obvious advantages over electronic voting. In many elections, there have been demands for a recount, which can only be possible with records of the individual votes. Paper ballots, punch cards and optically scanned ballots all meet this requirement. A physical trail is left behind to identify errors easily or to uncover trends in voting history. In addition, paper ballots are often very straightforward and can be understood by anyone using the ballot. The mechanisms behind paper systems are also easy to understand and easy to trace, while software, for instance, is not. As Karl Stephan observes, the mechanics behind a paper ballot do not require an expert to understand, whereas a piece of software does require one.

While paper voting systems have many advantages, they do not come without their own shortcomings. Manually counting paper ballots is an extremely slow process and is prone to errors. Punch cards can also be very problematic. Some produce hanging “chads,” which are tiny rectangular pieces of cardboard that are left hanging on the ballot. Counting machines

sometimes force the “chads” back into the hole and count them as a non-vote when they should have been counted as a vote.

Optical scanners also harbor many disadvantages. The printing on the ballots must be precisely marked for the scanner to count the vote. If a voter chooses to mark the ballot with an X or with circles, the scanner will not count the vote. Many voters may find the more complicated ballots difficult to follow and end up voting for too many or too few candidates ([LA Times](#)).

There are also many dangers that come with physical systems. They are prone to tampering and security infringements, and the integrity of the election depends on the accuracy of the count. Mechanical voting machines are large and clunky, with a total of 27,000 parts, and are so old that many of the parts are no longer made. These seem to be extremely complicated, which could imply that they are safe from mischief-makers, but it has been proven that they are very easy to rig with everyday tools. Physical vote-counting machines also have error rates of 0.01% to 0.1%, a range which, if correct, would produce as many as 100,000 mistakes in this country, where over one hundred million people vote in the Presidential election. This averages out to 2,000 votes miscounted per state, a larger margin than that by which George W. Bush won Florida in the 2004 Presidential election ([LA Times](#)).

In light of the problems with physical voting systems, it is obvious that a well-implemented electronic system has the potential to solve them all and more. In a perfect electronic system, there is no limitation to the design or layout of the ballot since it is displayed electronically. There is a potential for more intuitive layouts, vibrant colors, or perhaps even pictures and information about candidates. Programmers would be able to translate ballots

easily into many languages and a user or administrator could switch between languages easily and effectively. Along with display options comes the ease with which a system could be adapted to special needs. For example, it would be possible to increase the size of the text on the screen for voters with poor eyesight, or even to translate the ballot into an audio format for blind voters. Since paper is not required for the ballots, there will be a lessened economic impact and election officials will not need to estimate how many ballots they will need. It will also help election officials to provide for multiple ballot types in various kinds of elections such as primaries, general elections, and special elections (Bowen). Tabulation also benefits heavily from electronic voting systems. Counting the votes is instantaneous and there would be no need for recounts (Bonsor and Strickland). The chance for people to vote for too many or too few candidates would also be lowered because of built-in error-checking systems before the vote goes to tabulation (Bowen).

All of these potential benefits of electronic voting presume that the voting system, whether it be a DRE or an online election, is perfect. However, there are so many things that can go wrong with anything electronic that it is virtually impossible to maintain a perfect system. One fact is true of all software: programs will malfunction on a regular basis and sometimes the malfunctions are extremely subtle (Schneier). However, before even looking at the electronic security issues, it is relevant to consider drawbacks that are not related to security. There are four aspects of an e-voting system, an online system in particular, that would make it less attractive by its very nature: the susceptibility to coercion, vote selling and vote solicitation, and problems associated with registration (Rubin). Many things on the Internet are done in ways which do not provide a dependable method of enforcing the law. An

online voting system would make it very easy for people to be coerced into voting for a particular candidate. For example, in a traditional voting location, security and privacy are provided. However, in an online system, voters would cast ballots in places where they could be more susceptible to peers or strangers pressuring or forcing them to vote for a particular candidate. The opportunity for people to sell their vote would also increase, especially because it would be easy for a buyer to ensure that the voter casts his or her vote as the buyer wishes. With vote selling comes vote solicitation. It would become much more difficult to control solicitation by political parties at the time of voting. Registration is also a large issue, as allowing online registration would create new problems such as fraud (Rubin).

Electronic voting is further limited because of the nature of the medium. Even with a perfect design, the system could never be completely secure. In light of the problems with computers and technology in general, a new generation of personal computers would need to be created to ensure that an online voting system is absolutely secure. Stephan points out that a piece of software is very complicated and usually requires an expert to decipher. The programmer has many opportunities to install backdoors in the software to permit easy interference, given the right knowledge. Even without that occurring, there are many ways that an election could be electronically manipulated. It is very easy, for example, to install software that allows an attacker to control every aspect of a computer system remotely. This control could be so subtle that voters would think they had successfully completed a vote when in reality the attacker had changed their selection without their knowledge. In addition, "denial of service" attacks have become increasingly effective at disrupting service to many Internet users. If, for example, an attacker knew the general direction in which voters in a region would

cast their ballots, he could disrupt service to that area, thereby changing the outcome of the election to his liking (Rubin). Bruce Schneier of Counterpane Internet Security, Inc. summed up the problem nicely when he said, "A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers."

The many mishaps that have been seen in past elections reemphasize the risk of electronic voting. A strange and unforeseen error occurred in Volusia County, FL in the 2000 Presidential election that was won by George W. Bush. The final tally of the votes for candidate Al Gore in the county was negative 16,022 votes. A similar incident was recorded in Boone County, IA in 2003 when a DRE recorded votes totaling over 140,000 when the county has only 50,000 residents, with fewer than half of them eligible to vote (Schneier).

On November 7, 2006, elections were held in Florida for the U.S. House of Representatives. In Sarasota County, 18,000 ballots that were cast on electronic voting machines registered no votes. This resulted in an undervote of 16%, which is massive compared to the 2.5% undervote with paper ballots in that same election. In addition, the undervote rate for the Senate in all voting media was 1% in the same county. The candidate won by only 363 votes, a total which could have been easily altered by the missing 18,000 ballots (Lin and Espinoza).

In a similar case, Vivendi Universal held an electronic vote at its annual shareholders' meeting on April 24, 2002 to decide some pressing issues. CNN describes the meeting as "raucous" and reports that shareholders "jeered" at some of the issues the vote would decide. However, after the votes were counted by the system, the results showed an unusually high

abstention rate of at least 20% (“Vivendi: Hackers wrecked vote”). The usual abstention is only 3% to 4% (Verrier).

These problems are obviously not confined to one location or type of machine and are further illustrated by the fact that four California counties had difficulties with DREs in a March 2004 election. These included delayed polling place openings and miscounted and incorrectly marked ballots. In San Diego County, about one-third of the county’s polling places did not open on time because of battery problems caused by a faulty power switch (Hite).

Electronic voting is not without its own success stories. In 2000, Brazil became the first country to be rid of paper votes altogether and conduct an election entirely by this means. Similarly, in the 2003 French election to choose the representatives to the Assembly of the French Citizens Abroad, voters were given the option of using remote Internet voting. This resulted in over 60% of the votes coming in via the Internet rather than by the traditional paper votes (Lin and Espinoza). Also, in May 2004, India held an all-electronic vote for its 380 million voters. This turned out to be the world’s largest fully electronic vote to date. While it was far from perfect, it is generally considered a success (Weiner). While all of these elections worked nicely for the nation they occurred in, the United States is a different story. There are typically many more candidates on the ballot in the United States than, for example, in India. Therefore, a different solution is needed for the United States.

Many solutions have been proposed for the problems in electronic voting and it is widely agreed that, along with the other requirements of a public voting system, any solution must meet two basic requirements to be successful. First, DRE machines must have a voter-verifiable paper trail. This provides two safeguards: it will allow voters to confirm that their vote

was counted in the manner intended, and it will supply a mechanism for a recount if there are problems with the machines. In addition to the paper trail, security experts agree that the software used in a DRE must be open to public scrutiny. This would allow the public to inspect it and identify possible bugs so that they might be fixed. It would also improve voter confidence in the entire voting process, as it would lower the chances that an unfair system had been developed undetected (Schneier). In an attempt to improve voting systems in the United States, MIT is undertaking the "Voting Technology Project." This project will evaluate the reliability of existing voting systems and establish guidelines for their reliability and performance. In addition, MIT will present their own set of standards for any new voting technologies (Gallez).

Rebecca Mercuri, a computer security expert specializing in electronic voting security, has proposed a hybrid solution that combines the advantages of both paper and electronic systems. Referred to as the Mercuri Method, it seems to offer a good start in the search for a usable electronic system. The method requires that a paper ballot be printed containing the selections made on the computer. The voter can examine the ballot for correctness through a glass window or screen and deposit it in a ballot box. If, for any reason, the paper ballot printed by the machine does not match the intended choice of the voter, a poll worker would have the ability to void the ballot and allow the voter to try again. At the end of the election, the machine would have an electronic tally of the votes. This tally could be used for preliminary results, but the official count would have to come from the paper records produced by the machine. These ballots could be optically scanned for the tally and hand-tabulated in case of a recount (Mercuri).

It seems logical to conclude that fully electronic systems, whether via the Internet or DRE machines, are not yet ready to be used as the only method of voting in the United States. With current technology, it is impossible to create a completely secure electronic system that meets all the demands of a functional voting system. Until more research has been done and new technologies arise, electronic voting may be better left to less security-intensive situations than national or public elections. These may include shareholders' meetings, public policy initiatives, award nominations, opinion surveys, or school club elections. When choosing the next President of the United States, however, the American public must turn to a system that they trust. The physical nature of a paper ballot provides too much confidence to be cast aside as out-of-date. On the other hand, while a fully electronic system may not be the answer, e-voting provides too many benefits to be ignored. A hybrid solution, such as the Mercuri Method, seems to be the best possible voting method for the future.

### Works Cited

- Bonsor, Kevin, and Jonathan Strickland. "How E-voting Works." 12 Mar. 2007. HowStuffWorks.com. 12 Nov. 2008 <<http://www.howstuffworks.com/e-voting1.htm>>.
- Bowen, Debra. "Voting Systems FAQ." Ed. Debra Bowen. 2008. State of California. 12 Nov. 2008 <<http://www.sos.ca.gov/admin/about-the-agency.htm>>.
- "Electronic Voting." Wikipedia, The Free Encyclopedia. 30 Sep. 2008. <[http://en.wikipedia.org/wiki/Electronic\\_voting](http://en.wikipedia.org/wiki/Electronic_voting)>.
- Gallez, Florence. "MIT E-Voting Project To Analyze Experience Of Voters in Election." 30 Sep. 2008. MIT. 12 Nov. 2008 <<http://tech.mit.edu/V128/N43/evoting.html>>.
- Hite, Randolph C. "Electronic Voting Offers Opportunities and Presents Challenges." United States General Accounting Office. 12 May 2004. 12 Nov. 2008 <<http://www.gao.gov/new.items/d04766t.pdf>>.
- Lin, Gloria, and Nicole Espinoza. "Electronic Voting." Ed. Gloria Lin. 2007. Stanford University. 12 Nov. 2008 <<http://www-cs-faculty.stanford.edu/~eroberts/courses/cs181/projects/2006-07/electronic-voting/index.html>>.
- Los Angeles Times Staff Writers. "latimes.com: A 'modern' democracy that can't count votes." 11 Dec. 2000. CNN. 12 Nov. 2008 <<http://archives.cnn.com/2000/ALLPOLITICS/stories/12/11/latimes.votecount/index.html>>.
- Mercuri, Rebecca. "A Better Ballot Box?" IEEE Spectrum Oct. 2002: 46-50. 12 Nov. 2008 <<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01038569>>.
- Rubin, Aviel D. "Security Considerations for Remote." Communications of the ACM 45.12 (2002): 2+ . 12 Nov. 2008 <<http://avirubin.com/e-voting.security.pdf>>.
- Schneier, Bruce. "Schneier on Security." Bruce Schneier. 10 Nov. 2004. BT. 12 Nov. 2008 <[http://www.schneier.com/blog/archives/2004/11/the\\_problem\\_wit.html](http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html)>.
- Stephan, Karl. "Electronic Voting: Why or Why Not?." Engineering Ethics Blog. 18 Aug. 2008. Blogspot. 12 Nov. 2008 <<http://engineeringethicsblog.blogspot.com/2008/08/electronic-voting-why-or-why-not.html>>.

Verrier, Richard. "Vivendi Sees Signs of Voting Fraud." Los Angeles Times. 27 Apr. 2002. Los Angeles Times. 12 Nov. 2008 <<http://articles.latimes.com/2002/apr/27/business/fi-vivendi27>>.

"Vivendi: Hackers wrecked vote." CNN.com europe. 29 Apr. 2002. 12 Nov. 2008 <<http://edition.cnn.com/2002/BUSINESS/04/29/vivendi.hacker/index.html>>.

Weiner, Eric. "The Bombay Ballot: What the U.S. can learn from India's electronic voting machines." Slate. 29 Sep. 2004. Washington Post. 9 Dec. 2008 <<http://www.slate.com/id/2107388/>>.