The Future of E-Voting

Dev Ananda
Amanda Bui
Janet Gonzalez
Martha Prempeh

Information Technology and Public Policy

The Future of E-Voting

The Problem

Voting is an act of democracy. Citizens are given the opportunity to voice their opinions by voting. And although some feel that one vote doesn't matter, others feel that their vote is important and can determine the outcome of an election. And it might. How confident are we that our vote counts? Security, accuracy, ease of use, efficiency, and costs are aspects of voting to consider. If there is fault in any one of these aspects, is it worthwhile to vote? Would society benefit if improvements were made to the current voting systems? The arguments made in favor of paper ballots versus electronic ballots persist. Yet which one is more beneficial to society? And does this outweigh its costs?

2000 Election

In the 2000 National Election the famous "butterfly ballot" episode in Palm Beach, Florida sparked controversy for several reasons: (1) the ballot design, (2) the inconsistent election rules, (3) voter error, and (4) allegations of fraud. It is important to review what happen in 2000, because the election caused a dramatic wave for new laws to be implemented and it weighed the advantages/disadvantages of manual vs. electronic systems. To be able to analyze the problem, the individual has to know what are the threats, detection, correction, defense, vulnerability, of both systems. Technology is advancing, and in order to make that leap forward with electronic machines security issues need to be addressed. It's crucially important to remember that manual/electronic systems are not the only issue, but political parties, lobbyists, and the government also play a critical role to the problem.

Definition of Vote Fraud and Error

The amount of political power that is at stake could drive some potential elected officials to literally “fix” an election to favor their party. The question now becomes what system is more likely to prevent "fraud” from occurring and limit the chances of “error.” “It is not enough for elections to be accurate. We have to know that they are accurate” (Dill). Accuracy is the key, but it is difficult to get 100 percent of it if we have systems with flaws. The highlight of the 2000 election revolved around the question of whether “fraud” was committed in manual and electronic systems or was it possible that a random error occurred that accounted for all those under-votes and over-votes? We have to understand the difference between “fraud” and “error” in both systems. Fraud in manual systems deals with the tampering of ballots in order to change the intended vote of a voter. In electronic systems “fraud” is observed when there is tampering with the software/hardware and potentially using the computer code to change votes. Judge Burton, the Chairperson of the Palm Beach County Canvassing Board defined “an “error in the tabulation” as counting error in which the vote tabulation system fails to count properly marked or properly punched punch card ballots. Such an error could result from incorrect election parameters or an error in the vote tabulation and reporting software of the voting system” (Florida 2000 Election). The computerized counting machines in 2000 could have read the votes wrong and printed out a different outcome. So, if “error” or “fraud” occurred that evening is there truth to the statement that “Florida 2000 showed that it isn’t a matter of getting more people to vote for your candidate. Instead all you have to do is disqualify votes” (Florida 2000 Election). Fraudulent participants of both systems could have been political parties, partisan groups, lobbyist, corrupted poll officials, etc. It is difficult to detect or admit an incident of fraud because that would basically undermine our democratic electoral process. Some political

scientist believe that informing the public of an “error” is far less appalling than trying to explain to them that a fraudulent act has been committed by political actors.

Florida 2000

The inconsistent election rules did not help the situation in Palm Beach. The standards in Palm Beach County Canvassing Board were changed four times: First, dimples didn’t count. Then, the chad must be hanging from the ballot. Next, it was that a dimple would count as long as there is light coming through it. After that, any speck of light coming through would constitute a vote. Eventually, the courts put a stop to it and decided on the first standard. After all these different criteria, officials could have already implemented the other three standards before the court decided their final ruling. There was so much room for fraud and error to occur during that process, that it put the manual systems in a disadvantage. Then there was the Florida Court law that states “no paper ballot shall be voided...so long as there is a clear indication thereon to the election officials that the person marking such ballot has made a definite choice.” (101.011 paragraph 2) This means that election officials decided what is “clear and definite”, that level of discretion could have cause many problems.

Complications of Manual Voting

It is sometimes confusing to distinguish from fraud and error because an error could be committed by a voter, and later changed by any official, causing an act of fraud. For example, in the 2000 Election some individuals voted for both Gore and Bush (a situation known as an over-vote). The standards of Palm Beach County Canvassing Board stated the criteria that the dimples don’t count, that the chad must be hanging from a ballot. What if the poll officials said “well this voter looks like he wanted to voted for Gore but there is a dimple by Gore side and a hanging chad on Bush side; I believe that this vote was intended for Bush.” Is this

considered an error by the officials or fraud because the polling official made the candidate choice for him? Falsely interpreting a voter's intention is against the law, but how can those individuals be accountable when the systems themselves are not working? Many incidents occurred that evening that disqualified votes, changed votes, added votes, subtracted votes, and more. So, where draw the line between an "error" and "fraud" in both electronic and manual systems? After the manual recount in Palm Beach you had hundreds of people analyzing the ballots, the more people played with them the greater the chances of a chad falling out. Then it is counted as a vote, but a vote for whom? The person analyzing the ballot decides who the voter intended to vote for. Again the question is that "fraud" or just an "error".

Manual systems are very subject to voter error and that could potentially lead to fraud acts by political parties. In an event of a recount we set in the "human element" that could be potentially biased. A problem that is often ignored is the poll workers who have the ability to lose, hide, and destroy paper ballots without detection. Once the voting is over, and all the voters leave, how easy is it to access the ballots? The issues with paper ballots are the risks of over-voting, under-voting, hanging chads, etc. "Of the total 113,820 over-votes recorded in the ballot-data archive, nearly 25,000 were the result of confusing, poorly designed ballots, and most of them involved Gore, according to the most comprehensive examination yet of the more than 175,000 uncounted ballots from the 2000 Election."(Kunerth, Orlando Sentinel) On the other hand, electronic systems are less at risk of over-voting and under-voting. According to the article *Law and Date: The Butterfly Episode* written by Brady, Herron and other colleagues, the calculation of over-votes was over 19,000. When we are discussing potential "fraud", it is important to keep in mind that "the scale of attack needed to affect the outcome of an election depends on what proportion of voters favor each candidate. The more closely contested a

election is, the smaller the degree of tampering that would be necessary to affect the outcome." (Election 2000) This could be true in the year 2000, the presidential election was decided by 537 votes when George Bush proved victorious. According to the Election Incident Reporting system 4,417 incidents were reported in the state of Florida alone. If all those incidents were investigated, more shocking outcomes could have been displayed.

Detecting in electronic systems "...state and federal oversight and certification of voting software...security measures, such as election day monitoring, are available. Detecting an error or fraud in manual systems can be difficult if no one knows who to hold accountable. Professor Dill poses two levels of accountability: (1) can we detect error? and (2) can we correct it? In the 2000 Election there were hundreds of officials recounting votes; was there a high level of scrutiny establish by those who were observing them? The essential case is that manual systems could lead to many problems, especially if a recount is demanded. The aftermath of the 2000 election dealt with issues of fraud, error, over-votes, under-votes, hanging chads, etc. This election was critical because now we can view the advantages and disadvantages of different approaches to auditing for detection/ correction of fraud/error in manual vs. electronic systems.

Currents Downfalls to E-voting

Detection of "error" was found by the Hopkins Study that analyzed the Diebold's voting system and concluded "...that the code had serious security flaws that could permit tampering by persons at various levels, including voters, election workers, Internet "hackers," and even software developers." Then again, Diebold rebutted the accusations, and many computer scientists "criticized the study for not reflecting standard election procedures." (Mercuri) The disadvantage of electronic systems deals with "malicious computer code, or malware, that can often be written in such a way that it is very difficult to detect."(Thompson,

pg. 761). DRE software is somewhat complex, and the more complex it gets the harder it becomes to detect any unlawful modifications to the code. There has been solutions for these concerns by the National Association of State Election Directors (NASED), which has provided a program that uses "...an independent test authority (ITA) that test voting systems and certifies those that comply with the VSS. Testing ...by both hardware and software, and the tested software and related documentation is kept in escrow by the ITA." (NASED) To serve a correction on malware problems a great deal of attention needs to be place on computer code.

There has been several proposals by FEC to improve the security of DREs (1) ensuring that accepted security protocols are followed appropriately, (2) improving security standards and certification of voting systems, (3) use of open-source computer code, and (4) improvements in verifiability and transparency. Also, in DREs, the ballots could be displayed by allowing voters to click a page to translate their ballot into the language they feel more comfortable using. This can prevent "error" by detecting the problem of language barriers and correcting it. In manual systems it is a tedious task to ask someone for help and sometimes no one will offer to help. Before casting your vote in electronic systems, there is a page that is brought up to review your inputs. That way if there is an "error" that the voter made it could be corrected by the voter, before their vote is finalized. It gives the individual a second chance to go through it. Another recommendation of "parallel monitoring" is presented for detecting error by using a system "in which selection machines are tested while in actual use on Election Day to determine if they are recording votes accurately." (FEC)

Integrity and Accountability are two of the key points Professor Dill spoke about. A way to protect the integrity of electronic systems and correct possible "fraud" or "error" is by using Cryptography. "Cryptography is important not only in making it difficult for unauthorized

persons to view critical information (security), but also in making sure that information is not changed or substituted in the process of being transferred (verification).” (NRC, p. 301-310) This is one of many suggestions for correcting the downfalls of electronic systems. Auditing transparency in the DREs we currently implement is skeptical because “the actions that occur between ballot screen and the final vote tally are not subject to human observation.” (FEC) This is why DREs are nicknamed the “Black Box”, but then again we viewed the human observation of the “butterfly ballot” episode and that did not cause a great amount of transparency either. The federal Voting System Standards (VSS) also “...point to the lack of proven case, despite many accusations, of election fraud involving computer tampering.” (CRS-22)

Auditing in DREs can include “engineering the DRE so that it creates a log of all actions performed, especially those that might indicate tampering. It can also include the creation of an audit trail for votes.” Cryptographic protocols and HAVA to an extend provides a way for auditing, but malware can also pose a threat to auditing. If there is an “error” or “fraud” that is done to the software, then the question of what votes would be counted will arise.

Detection

Detection is having knowledge of when an attack is occurring at the present moment or an attack that was already attempted. A correction in manual systems could be difficult if “...Florida law only gives counties the option to use manual counting if there was an error in tabulation (i.e. a broken machine or fraud, etc.) Further, even if an error is found the canvassing board has the option of “fixing it” and continue counting ballots by the machine.” Correction always works side by side with detection, if a great potential “error” is occurring but the laws of counties have stipulations of when to use correction then the problem may not be fixed. After the 2000 election there was substantial data collected that detected “error” due to

ballot design. Now there have been many corrections of manual systems to try to prevent chaos to occur like it did in 2000. After all the uncounted votes of the 2000 National Election"...HAVA requires that voters be notified of over-votes before a ballot is cast and be given the opportunity to correct error. However for systems where this is not possible...an education and instruction program is permitted." This is another example of correcting future errors from occurring due to bad ballot designs. The disadvantages of manual systems trace back to the recounts of votes in the 2000 election. "Recounts have received criticism because of non-uniform and untested methods for re-evaluating what constitutes the intention of a voter (Bush v. Gore)" (Walter, p.4)An advantage of manual system detection has to do with "the method of outlier detection that has been successful in identifying a number of anomalous votes outcomes... in Florida for the 2000 U.S. presidential election, where we demonstrated that the vote for Reform candidate Pat Buchanan in Palm Beach County was produced by processes substantially unlike the process that generated his vote throughout the rest of Florida." (Walter, p. 9)

Administration

"The administration of election is a complex task, and there are many factors involved in choosing and using voting system in addition to security. They include factors such as reliability, propensity for voter error, usability, and cost...election administrators must consider them in decisions about what systems to use and how to implement them." The DRE code has been criticized by many as a bad design, but so has the "Butterfly Ballot" in the manual system used in Palm Beach. There has to be security policy that is implemented that could function for both systems. There are advantages and disadvantages with electronic/manual systems and in order to choose the best one, individuals have to outweigh the consequences.

2004 Election

A lot of federal funds were invested prior recent 2004 national election to replace outdated mechanical and paper-based voting systems. This trend, accelerated by concern over the failures of the 2000 election, spurned the wide use of electronic voting in 2004's Presidential election. However, many experts in the field believe that these technologies are being rushed too quickly into use, without proper verification and preparation for tampering, malfunctions, and security. How successful was e-voting in the 2004 election? Through an in-depth case study of this year's election, I will be examining the companies, research institutions, financial investment, outcomes, successes, problems, concerns, and controversies specifically involved in the 2004 national presidential election.

Errors

While the disorder of Florida's national election in 2000 spun a flurry of electronic voting system implementation around the country, this has proven to be faulty. For example, an error in the Gahanna precinct of Franklin county, Ohio caused the machine to record over 3,893 extra votes to President Bush. The reading was 4,258 votes for Bush and 260 for Kerry. However, records show that only 638 votes were cast in that precinct. Zero votes were recorded for a county commissioner race on the same machine. These electronic voting machines require high maintenance and upkeep. Some of the machines could not boot up properly on election morning because they were overcharged. These machines were made by Danaher Control ELECTronic, and the machines of many other companies have been known to malfunction as well. For instance, polling officials were told by Unilect, whose machines were used in a North Carolina county, that the machines could hold 10,500 votes. In actually, the machines only held 3,005, which resulted in 4,500 votes being completely lost. Similarly, there was a malfunction in the San Francisco municipal office positions. A glitch in the software

prevented the ranked-based system of voting to produce the results. The San Francisco Department of Elections Director John Arntz reported “All the information is there. It's just not arriving the way it was supposed to.”

There are many types of errors that could happen. This is all the more dangerous because there is no paper or voter verifiable audit trail. When one votes on paper, they see the product of their action right on the paper, and it is proof that they will hand in the vote they intended. However, computers are not that transparent. Without a paper receipt, voters have no way to know that the input they put on the screen was recorded properly in the computer memory banks. The obvious mistakes, like a machine giving a candidate thousands more votes than the 365 he was supposed to have, are a lot less harmful than the little mistakes. Because they are easily recognizable, they can easily be fixed. However, tiny discrepancies can go unnoticed, especially without an audit trail. If every computer records even a few votes wrongly, in an election as close the 2004 election, where many states were close to a 50-50 split, a candidate is capable of being wrongly elected. Professor Dill suggested in his October 17, 2004 lecture, all aspects of the election should be publicly observable or independently checkable, or ideally both. It is not enough to trust that elections are accurate or very close to accurate. There must be a reliable way to check, prove, and monitor before such voting systems are ready for use. Detection is the first step to repair. Currently, the accuracy of Direct Recording Electronic systems is based on trust alone.

In addition, according to a UC Berkeley statistical study, counties in Florida that used electronic voting had a higher discrepancy between exit polls and statistical predictions that those that did not. Another threat to the accuracy of elections is hacking, or deliberate tampering with the electronic system. This is a very real possibility for several reasons. One, the votes are

not kept in locked boxes with only one key that can be assessed from only one place like paper votes, but instead they require electronic passwords. If a hacker had this information, he would be capable of tampering with an election from anywhere with the help of the internet. Similarly, it is not as easy to spot electronic tampering as it is to spot paper tampering. As Professor Dill mentions "Everyone understands paper." Not everyone, including poll worker and election officials and watchers understand information technology.

There are many motives to be a hacker, and thus the security risks are great. For example, trillions of dollars in business assets are at stake in this election. Diebold, a company known to be a heavy Republican campaign supporter, is the leading company in electronic voting systems. Candidates themselves have been known to tamper with election, for example President Nixon and the Watergate scandal, as well as political zealots. Random bugs and intentional viruses are the biggest risk. There should be much more security than there was for the 2004 election.

So it appears the prevalence of electronic voting system has not fixed the kinks which made the 2000 election so controversial, but may have actually made the situation worse. In the rush to implement these machines, the security and reliability of this technology was not adequately ensured. The brewing controversy over the 2004 national election has proven that sometimes, the cure can be more harmful than the condition.

Results Debate

The full scope of the effect of electronic voting on 2004's national election is yet to be fully known. As of now, there are two sides to the debate, one that feels that e-voting technology was not secure enough to be used nationally in such an important election, and one side that feels the warnings and speculations are exaggerated. Two election protection groups

have issued papers on the abnormalities of the election this month. Common Cause published Report *from the Voters: A First Look at 2004 Election Data / Common Agenda for Reform* and co-hosted a forum in Washington, DC on "Voting System Problems". In addition, the Election Protection Coalition published *Shattering the Myth: An initial Snapshot of Voter Disenfranchisement in the 2004 Elections.* These reports suggest that severe error and even fraud may have been involved in the national election. A UC Berkeley statistical study found that there were significant discrepancies between exit polls and result prediction in Florida's election, but failed to make any political conclusion. This and other studies have been contested by a MIT / Cal Tech report and a Drexel University study that concluded that the irregularities are normal and that e-voting has been successful, considering the margin of error in any national voting system.

Florida 2004

This time around, Florida is again a hotspot of election controversy. As recounts requested by Ralph Nader are being ordered in Ohio, Florida also appears to be next on the lists, with a number of suspicious discrepancies. In the final count, Ohio gave Kerry 18,00 more votes than the original count. While critics may point to the fact that Florida's governor through both the 2000 and 2004 election was George Bush's brother, Jeb Bush, and that ironically the errors of both national Florida elections settled in George Bush's favor, others warn not to jump into conspiracy theories. Nevertheless, it has been concluded by several political organizations that "a million African-Americans were disenfranchised in the last election" and that a similar situation may have happened in 2004. Since the Civil Rights Movement, over 85% of African Americans vote democratic.

2004 Final thoughts

In conclusion, this election may prove to be just as controversial as 2000's national election on the validity of voting systems. Ironically, the debate in 2000 centered on the inefficiency of paper systems, while 2004's debate will center around security and possibly, fraud. The issue of election validity is especially important and sometimes taken for granted in a developed democracy like that of the United States. As Kevin Shelley, California Secretary of State reminds us, "The core of our American democracy is the right to vote. Implicit in that right is the notion that vote be private, that vote be secure, and that voted be counted as it was intended when it was cast by the voter. And I think what we're encountering is a pivotal moment in our democracy where all of that is being called into question" (VerifiedVoting.org).

Policy

Current e-voting policy varies from nation to nation, with many experimenting with new methods to implement it in practice. American e-voting policy begins fundamentally in how the U.S. Constitution delegates authority on election processes. States are given the power to regulate election proceedings. This includes a number of responsibilities including registration, absentee voting, polling locations, counting votes, as well as paying for the elections process. In many cases, the decision of how elections are administrated is delegated to even more local levels. Debate around e-voting policy revolves around a few key laws that have come to shape the future of e-voting in the United States: (a) Help America Vote Act (HAVA); (b) Digital Millennium Copyright Act (DMCA); (c) Uniform Computer Information Transactions Act (UCITA); (d) Voter Confidence and Increased Accessibility Act of 2003.

Help America Vote Act

The Help America Vote Act, created as a response to the messy United States presidential election in 2000 (Bush vs. Gore), has number of implications for e-voting policy.

First, the act appropriates almost $4 billion to update the elections process and $325 million to the updating of outdated voting technologies and systems. Second, it attempts to extend voting accessibility for other voter groups. The law mandated that an updated process must exist to provide provisional voters access by 2004 as well as access for disabled persons by 2006. The law also stipulates that there must be at least one DRE (direct recording electronic) machine per county. The law, however, leaves it up to the states to decide how they will comply with the terms of HAVA. The act does not establish what types of technologies to use, nor how many there should be per precinct. In general, there have not been any national requirements for electronic voting set by the federal government, and some states that have already invested in technology for future elections fear that new standards may cause millions in wasted money (NIST Website).

Digital Millennium Copyright Act

The Digital Millennium Copyright Act affects e-voting policy in a few inconspicuous ways. As it applies to e-voting, the DMCA makes reverse engineering practices that were previously legal under fair use terms now prohibited. With a deluge of vendors attempting to sell their electronic voting equipment to states, the law essentially makes it illegal for interested parties to explore the functions of the equipment, and ensure the correct operation of the equipment as guaranteed by the vendor. The importance of this act resonated strongly when 2 students at Swarthmore College, posted links to several thousand technical support memos, along with source code information of e-voting technology developed by Diebold systems. Bev Harris of Black Box Voting, Inc., who has become an icon of for voter integrity, first encountered the materials online. The memos suggested wrongdoing by Diebold systems, including software flaws, which manufactured systems used in Florida for the 2000 election,

prompting public skepticism as about the legitimacy of the Florida elections. When alerted at the public access to company records, the company soon threatened legal action under the DMCA. However, Diebold was recently found guilty of threatening DMCA infringement and ordered to pay damages to the two Swarthmore students, while other ISP service providers, with the support of voting activist organizations, have continued to resist Diebold's complaints.

Uniform Computer Information Transactions Act

The UCITA was developed by the National Conference of Commissioners on Uniform State Laws. This law allows many protections that have a direct impact on e-voting in the United States (NIST). First, it places restrictions on the ability of consumers to publicly comment or criticize flaws in the technologies. Furthermore, along the same lines, it sheds liability for companies selling software that has clear shortcomings in function, allowing the aforementioned product suppliers to sell their product despite noted flaws. Thus, the law, for e-voting, essentially protects misconceived e-voting technologies from being denounced in any way. The law also allows "back-door" entrances to software and other technologies, permitting unauthorized users to manipulate the functioning of the equipment, which is certainly a threatening feature, in terms of the maintenance of legitimate elections.

Voter Confidence and Increased Accessibility Act of 2003

Finally, the proposed Voter Confidence and Increased Accessibility Act of 2003, if passed would require any voting system to produce a voter-verifiable paper ballot of systems participating in government elections. Democrat representative Rush Holt of New Jersey proposed the bill, citing a need for more accountability and confidence in the elections process. Many large groups, organizations, and scholars are in favor of stronger regulations on voting

accuracy and privacy and these names head a list of advocates and cosponsors for the Voter Confidence and Increased Accessibility Act of 2003.

Actors

There are a number of principal actors that mold and guide the agenda of e-voting in the world and in the U.S. These forces can be primarily attributed to several key groups, whose interest revolves around electronic voting, other than the public in general: (a) current and potential voting technology and services vendors; (b) government commissions and committees, whose aim is to resolve and improve election administration and processes; and a blend of (c) voter and election rights organizations and advocacy groups and (d) non-profit organizations, scholarly researchers, and projects who aim to find better ways of conducting electronic voting, protecting voter privacy, and ensuring legitimate election outcomes.

Vendors

After the enactment of HAVA, the number of voting technology vendors and service providers grew substantially, competing to provide voting software and machines to newly endowed states and counties. Some states proceeded rapidly on e-voting funds appropriated by HAVA, purchasing and updated voting machines. However, alarmed at the potential complications, flaws, and security threats, voter rights groups and academic circles alike campaigned against current e-voting methods (such as DRE machines) until open technical standards were determined. The three largest electronic voting system and services vendors are Diebold Election Systems, Sequoia Voting Systems, and Election Systems & Software. Many issues were raised when Johns Hopkins researchers found widespread security flaws in the publicly published software memos of Diebold Election System. Recently, six leading vendors have collaborated with the Information Tech Association of America (ITAA) to form the trade

group Election Technology Council (ETC). Members of the ETC defend election technology as an evolving industry in which new standards and certifications will necessarily arise. Sympathizers also cite the fragmentation of the new industry as a safeguard against manipulating elections, while others charge that electronic voting machines are "no more vulnerable than electronic scanners of paper ballots (Gross)" Cautious of public criticism of other leading vendors of DRE devices (Sequoia, ES&S) as well, new vendors have sought to provide updated systems with verified voting capabilities that are now demanded in California, for example.

After the implementation of HAVA, a renewed effort on the part of the government to legitimize and safeguard future elections followed. Congress first placed the responsibility of e-voting implementation in the hands of the National Institute of Standards and Technology (NIST).

Government Commissions

The Election Assistance Commission (EAC) was put in charge of assisting state and local governments transition towards more e-voting devices under HAVA. The commission, supported by the National Institute of Standards and Technology (NIST), includes the Technical Guidelines Development Committee (TGDC), which "makes recommendations to the EAC on voluntary standards and guidelines related to voting machines." NIST is an arm of the Commerce Department, which was authorized under HAVA to improve voting systems across the country. The NIST agency, by means of its Information Technology Laboratory (ITL), have these basic objectives, according to the NIST website: chairing and managing the TGDC, providing research and recommendations to the EAC and TGDC, technical guidance, testing, and establishing generally accepted standards. The current standards were established by the Federal Election Commission in the 1980's, but represent an outdated model which current

experts are attempting to supplant. Thus far, NIST has done much by fostering discussion, creating an international symposium, as well as a new comprehensive report to Congress on human influence on voting technology, updating a previous report issued by the FEC. NIST was funded $500,000 in 2003, and has continued work, despite budget reduction via its own funds (NIST website).

Advocacy Groups, Researchers, and Projects

As one of the most hotly contested debates in information technology policy, e-voting has generated an immense amount of interest in the discussion of technology, security, legitimacy, turnout, and numerous other topics related to voting policy in this country and around the world. E-voting has been a substantial topic in voting policy for the last decade or so, culminating recently with a flood of research that has ignited debates over its applicability in current voting systems. Scholars range from applicable disciplines in: computer science, engineering, political science, law, philosophy, and numerous other fields that are involved in the multitudes of aspects that comprise electronic voting.

E-voting has spurred many projects, websites, weblogs, and other organizational structures that have created a strong online community, filled with a wealth of information about e-voting. Scholars such as David Dill, Lorrie Cranor, Louise Ferguson, and Douglas Jones run websites that provide expert analysis and technical information that is pertinent to the debate. Some colleges, in conjunction with researchers, have also furthered the field, such as the MIT-CalTech Voting Project, and reports published by Johns Hopkins and UC Berkeley, among others. Websites like www.evoting-experts.com offer extensive commentary by leading minds in the field as well. In addition to the wave of academic guidance offered by so many experts, in the field, discussion of e-voting also involves various advocacy groups that aspire for different goals.

The Electronic Frontier Foundation (EFF), for example, is a membership organization dedicated to protecting civil liberties in the increasingly digital age and contributing to the public discourse. Other groups such as Black Box Voting, run by Bev Harris, are activist in nature, finding abuses and flaws in a system that is not widely understood in the public. Some organizations seek to provide information and affect policy by suggesting reforms such as the paper audit trail system, supported fiercely by organizations like VerifiedVoting, founded by David Dill.

Is It Worth?

Electronic voting proves to be a promising alternative to paper ballots. Yet problems still persist about how much faith we should put into the electronic voting systems as we are unsure if possible glitches may take place. In November 2000, the presidential election was decided by 537 votes. And after this November 2004 election, it was uncovered that President Bush had been given 3,893 extra votes in a county where only 638 ballots were cast. Although the extra votes and the glitches in the electronic voting system could not have been enough to change the election's outcome, there rests uncertainties about the security and accuracy of electronic voting. It is not enough for electronic systems to be accurate; we have to know this.

People, Process, and the Technology

What contributes to the success of the overall election process depends on three things: the *people*, the *process*, and the *technology*. And the fact that there is criticism about electronic voting is based, partially, due to the fact that people are more comfortable with paper ballots. The reason for the push for paper ballots is that it is a "transparent" process. It is permanent, it can be viewed by the public and most importantly, everyone understands paper

(Dill). Any new system must be as trustworthy as the paper ballot. And the main concerns are whether we can detect error in the system and whether or not we can correct it from thereon.

With direct recording electronic voting machines, you are relying on electronic records to be the true records of ballots that have been cast. And direct recording electronic systems has its pros and cons. The benefits of direct recording electronic systems include the fact that it can accommodate persons with various disabilities and provide features that protect against common voter errors. However, the negative aspects include the cost and lack of an independent paper audit trail. In addition to this, in the electronic voting system, there is always the risk of bugs in the system. And it is impossible to find all the bugs as it is usually the unpredictable and nasty bugs that remain. But bugs are not the only problem with electronic systems. With optical scan voting equipment, the benefits of using this type of voting device include the cost and enhanced security associated with having a paper audit trail. However, the negative aspects include lower ease of use, limited ability to accommodate voters with disabilities.

Susceptibility

There is also the problem of potential attackers, whether they be hackers, candidates, zealots, or a foreign government; the fear is that there is someone or group who is sophisticated and financially secure enough to manipulate election results. "In Broward County…Bush appears to have received approximately 72,000 excess votes…these effects are not attributable to chance" (Verton). This study, by researchers at the University of California, Berkeley argues that in the recent election, President Bush was given an excess of 130,000 or more votes. It also goes on to state that "Counties with electronic voting machines were significantly more likely to show increases in support for Bush between 2000 and 2004

compared to counties with paper ballots or optical scan equipment." It is without a doubt that the electronic voting system is a system with flaws.

However, the electronic system is not the only problem; another problem we encounter with voting systems is the people involved with the voting process. In one North Carolina county, more than 4,500 votes were lost in the 2004 election because officials mistakenly believed a computer that stored ballots electronically could hold more data than it did. With problems like this occurring, it is hard for voters to put complete confidence in the system.

A solution to this problem includes making it so that it is publicly observable and independently accurate. And the best way to detect error is by making sure the system is made to be perfect. It must never lose or change votes. But a question that remains: is our current computer technology up to this task? There are obviously benefits and disadvantages to using electronic voting systems. Again, the problem is that as we search for new solutions to replace the older equipment used for elections, we face uncertainties and possible faults with the newly introduced electronic voting systems.

Usability

And other things to consider are outside variables, which include size of jurisdiction and languages spoken by voters and performance of voting system used. The criteria which we need to use in order to find the solution to the current voting problems must be focused around quality and it must be ensured that there is perfection with the system. There must be checks and testing on the system to make sure it performs as intended and that there is system implementation. And there also must be training available to those involved with overseeing the voting process; it must be standard that these people have the right knowledge and skills to

operate and use the system. There also must be a well-defined and understood process governing this operation and use.

Near term challenges it faces include performing security, testing, and maintenance activities that it needs to operate as intended. In addition to this is the concern with managing the system, the people who interact with the system, and the processes that govern this interaction as interrelated and interdependent parts. Long term challenges include having reliable measures and objective data to know whether the system is meeting the needs of the user community (both voters and those that administer the elections).

Specific concerns with electronic voting deal with its security, accuracy, ease of use, efficiency, and its cost. Problems with any of those aspects could mark electronic voting as an unreliable source for voting. As for optical scan and DRE systems, both are claimed to be highly accurate. Ohio's example of an error due to the electronic voting system suggests mechanical error. However, in 2001, vendor surveys showed between 99-100 percent accuracy of vendors of DREs. There are glitches within the electronic voting system; however, it proves to be accurate the majority of the time.

Making choices about future system changes must also put into consideration whether these costs of new technology are affordable. However, we must view the social benefits to electronic voting. Electronic systems may stop a voter from choosing too many candidates or too few candidates in a race. You must also acknowledge the fact that with electronic voting systems, there is no room to tamper or falsify physical ballot results.

Electronic voting is a benefit to society, if it is tested correctly and made so that it will not malfunction. This is why Congress enacted the Help America Vote Act (HAVA) of 2002 which established the Election Assistance Commission (EAC) to assist in the

administration of federal elections. The act also established a program to provide funds to states to replace older punch card and mechanical lever voting equipment. Improvement is necessary and this act helps to improve election administration, improve accessibility, train poll workers, and perform research and pilot studies. Specifically was created for fundamental election administration reform, and the government even authorized for $3.86 billion in funding over several fiscal years for programs to be established for this improvement.

Validity Over Affordability

We are faced with a situation. There are benefits and disadvantages with paper ballots. And there are benefits and disadvantages to electronic ballots. This is why we offer these alternatives to be considered.

1) Only use paper ballots. This would make it so that we rely on the humans; those who we can hold accountable for keeping manual records of votes.

2) Give the option of either paper ballots or electronic. This would make it so that people who are more comfortable with paper ballots can use this system. Yet this would also accommodate those with trouble using paper ballots, for example, the deaf or blind.

3) Give the option of paper or electronic, and additionally offer the option of internet voting. The Internet, as an option, would be evolutionary. But because we are faced with problems with our current voting systems, it would be too big a step forward to try internet voting.

We suggest option number 2—to maintain our current voting systems. Investing in this option would allow voting precincts to accommodate a wider range of people. But in doing so, we have to make sure there are standards—we must get technology to meet these standards nationally for it to be properly implemented. It is important to put into account the

different problems dealing with voter systems and to ensure its effectiveness. It is evident that buying DRE units is more expensive than buying optical scan systems. However, being able to purchase touch-screen DRE units for individual precincts can accommodate the blind, deaf, and paraplegic voters. And by investing in electronic voting systems, not only does it accommodate more people, it maintains ease of using, and it can protect from common errors. Particularly, costs vary depending on the requirements of individual jurisdictions. And in the end, the costs are about $3 billion. Despite this, it is still more beneficial to society to invest in electronic rather than paper ballots.

References

Journals:

Geisler, G. (1993). Fair? What's fairness got to do with it? Vagaries of election observations and democratic standards. *Journal of Modern African Studies*

Mebane, W. (2003). Detecting and Correcting Election Irregularities.

Hite, R. C. (2004) Elections electronic voting offers opportunities and presents challenges.

Thompson, K. (1984). Reflections on Trusting Trust *Communications of the ACM 27,* 1984

Electronic:

Cranor, L. (2004). Electronic Voting Hot List. Retrieved from http://lorrie.cranor.org/voting/hotlist.html

Dill, D. (2004). E-voting Misconceptions. Retrieved from www.verifiedvoting.org/article.php?id=2609.

Dill, D. Lecture, October 14, UC Berkeley.

Dugger, R. (2004). How They Could Steal the Election this Time. *The Nation*. Retrieved from www.thenation.com/doc.mhtml?i=20040816&s-dugger, July 29, 2004.

Gross, G. (2003). E-voting Vendors Seek Credibility." *PC World*. Retrieved from http://www.pcworld.com/news/article/0,aid,113823,00.asp>

Jones, D. "Voting and Elections." Nov 2003. University of Iowa. 3 Dec 2004. http://www.cs.uiowa.edu/~jones/voting/

Mercuri, R, "Critique of 'Analysis of an Electronic Voting System'document," 24 July 2003 http://www.notablessoftware.com/Papers/critique.html

Suchetka, D. (2004). Final Count in Ohio Give Kerry 18,000 More Votes. *VerifiedVoting.org,* www.verifiedvoting.org/article.php?id=5398, December 3, 2004

Verton, Dan
"University researchers challenge Bush win in Florida" November 18, 2004, from http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,97614,00.html

Zetter, Kim, “Florida E-vote Study Debunked”, *Wired News*, www.wired.com/news/evote/0,2645,65896,00.html.

E-Vote Glitch Inflates Bush Total
http://www.wired.com/news/evote/0,2645,65609,00.html?tw=rss.TOP

Frequently Asked Questions about DRE Voting Systems, *VerifiedVoting.org*, www.verifiedvoting.org/article.php?id=5018.

Manual Recount Procedures and Partial Certification of County Returns
http://jurist.law.pitt.edu/election/de00_13.html

National Institute of Standards and Technology. Dec 2004. www.nist.gov

National Committee for Voting Integrity. <votingintegrity.org>

Secure Electronic Voting http://www.loc.gov/catdir/toc/fy034/2002040608.html

Voter Protection Groups Release Election 2004 Reports.
www.verifiedvoting.org/article.php?id=5421.