



ELECTION FRAUD

In today’s highly charged political environment close elections are breeding grounds for post-election suspicion. These suspicions are based on the theory that even a small amount of deliberate fraud, accident, mishap, or improperly followed procedure might have tipped the election the other way. While the presidential election of 2000 is perhaps the most salient example, outcomes in other close races have been very closely scrutinized for irregularities by supporters of the losing side (Celeste et al. 2005).

There are several important questions that this white paper seeks to answer: What constitutes election fraud? What evidence is there, if any, of election fraud with our current voting systems? What procedures can be used to continue to ensure the accuracy and security of our elections? Specifically, this paper will discuss election fraud as it applies to electronic voting devices and paper ballots.

Attitudes about election fraud, and the causes of alleged fraud, depend in part on which political party is in charge or whether your side won or not. Republicans believe there is rampant voter fraud in Democratic strongholds – big cities and minority neighborhoods (Follman et al 2007; Nather 2007). Democrats claim that Republican electoral reforms, like requiring voters to show photo ID, do not prevent fraud, but rather suppress Democratic voter turnout on Election Day. “No election system is ever good enough for the candidate who loses the election,” states John Lindback, Director of the Elections

Division for the Oregon Secretary of State (Wildermuth 2007).

Rumors and accusations of election fraud abound. Bloggers, editorials, and pundits of all political leanings claim that electronic voting systems, and therefore elections, cannot be trusted and that democracy is in danger. Public paranoia over electronic voting has become widespread. However, it is necessary to put the current concerns about electronic voting into perspective by remembering that every type of election system is subject to fraud and errors.

History

Historically, local political parties have played an important role in perpetrating election fraud. Elections were often controlled by local party organizations, making it easy to destroy, miscount, or falsely multiply ballots. The key motive for fraud was the immense local patronage benefits afforded to winning parties, such as owning lucrative franchises, running police and fire departments, setting utility rates, or building large-scale public works. Today, local political party organizations are much weaker, in part because of their limited access to such widespread influence (Minnite and Callahan 2003).

Paper ballots were much abused in the late 19th century. In 1892 Jacob H. Myers invented the lever voting machine, claiming it could “protect mechanically the voter from rascaldom, and make the process of casting the ballot perfectly plain, simple and secret.” Lever voting machines were in widespread use by the 1930s. Political bosses in Chicago and other places soon learned how to add votes by turning the wheels at the back of the machine, leaving no evidence of their handiwork. Punch-card machines and optical scanners replaced lever machines in the 1960s in many jurisdictions. These newer machines had problems with the subjective reading of improperly filled-out ballots in order to clarify voter intent. The paper ballots could easily be altered or voided while they were transported to a central counting station. The latest technology, direct electronic recording (DRE) voting

devices, bring with them a separate set of concerns, including the possibility that unscrupulous programmers could manipulate the new machines (Fund 2004; Shamos 2007). However, as modern election administration has become more sophisticated, fraud has become more difficult to pull off.

Over the years, media reports have recorded a large number of *allegations* of election fraud. These reports are enlightening in three areas (U.S. Election Assistance Commission 2006):

- Regarding the pervasiveness of complaints of fraud and intimidation throughout the country.
- The correlation between fraud allegations and the perception that the state was a “battleground” or “swing” state.
- The fact that there were reports of almost all types of voting fraud and voter intimidation.

However, these news stories provide much less information as to whether the allegations were ever formalized as complaints to law enforcement, whether charges were filed, whether prosecutions ensued, and whether any convictions were made. Nor do they provide much data as to the number of complaints, charges, and prosecutions of voting fraud and intimidation throughout the country.

What is Election Fraud?

In its simplest terms, “election fraud” means fraudulent or deceptive acts committed to influence the act of voting. Too often, other forms of election misconduct or irregularities are improperly labeled as fraud when, in fact, they are due to technological glitches, mistakes by election officials or voters, misconduct by individuals other than individual voters, and a host of other problems (Whitehead 2008).

Election fraud involves a substantive irregularity relating to the voting act – such as bribery, intimidation, or forgery – which has the potential to taint the election itself. Simply put, election fraud is conduct intended to corrupt any of the following (Donsanto 2006):

- The process by which elections are conducted and ballots are obtained, marked, or tabulated;
- The process by which election results are authenticated and certified; or
- The process by which voters are registered.

Election fraud is the basis for federal prosecution under a number of United States statutes. According

to Craig C. Donsanto, Director of the Election Crimes Branch of the U.S. Department of Justice, most election fraud is aimed at corrupting elections for local offices, which control or influence government-related jobs and contracts (known as patronage). Election fraud schemes are thus often linked to other crimes such as protection of illegal activities, corruption of local governmental processes, and patronage abuses.

A wide variety of potential election, or voting, fraud has been reported in the media, including (U.S Election Assistance Commission 2006):

- Absentee ballot fraud
- Voter registration fraud
- Voter intimidation and suppression
- Deceased voters on voter registration list and/or voting
- Multiple ballots from a single voter
- Felons voting
- Non-citizens voting
- Vote buying
- Deceptive practices
- Fraud by election official

According to the EAC, election crimes generally fall into one of four categories: acts of deception, acts of coercion, acts of damage or destruction, and failures or refusals to act. In their 2006 report, the Election Assistance Commission (EAC) defines election crimes as:

...intentional acts or willful failures to act, prohibited by state or federal law, that are designed to cause ineligible persons to participate in the election process; eligible person to be excluded from the election process; ineligible votes to be cast in an election; eligible votes not to be cast or counted; or other interference with or invalidation of election results.

Election crimes can be committed by voters, candidates, election officials, or any other member of the public who desires to criminally impact the result of an election. However, crimes that are based on intentional or willful failure to act assume that a duty to act exists. Election officials have particular assigned actions and for the most part clearly defined duties with regard to elections. By and large,

other groups and individuals do not have such duties (U.S. Election Assistance Commission 2006). Most instances of election fraud involve voter registration, voter intimidation and suppression, multiple voting, felons voting, and absentee ballots.



Election fraud is a serious crime that can be prosecuted at the federal and state levels. The penalties carry fines and lengthy prison terms. In some states, a person convicted of voter fraud can permanently lose the right to vote (Minnite and Callahan 2003).

Over the last forty years Congress has enacted new criminal laws to combat fraudulent voting. Subsection 1973gg-10(2)(B) of the Voting Rights Act of 1965 prohibits any person, in an election for federal office, from defrauding or attempting to defraud the residents of a state of a fair election through casting or tabulating ballots that the offender knows are materially false or fraudulent under state law. The focus of this provision is not on any single type of fraud, but rather on the result of the false information: that is, whether the ballot generated through the false information was defective and void under state law. This subsection of the statute applies only to elections that include a federal candidate. However, fraudulent activity aimed at any race in a mixed election (federal and local races) has the potential to taint the integrity of the federal race (Donsanto 2006).

For the purposes of this white paper, the definition of election fraud is confined to knowingly and willfully depriving, defrauding, or attempting to deprive or defraud the residents of a state of a fair and impartially conducted election process. This includes activities such as:

- Diluting valid ballots with invalid ones (ballot box stuffing).
- Rendering false tabulations of votes.
- Preventing valid votes from having an effect in an election.

- Fraudulently altering or changing the vote of any voter, thereby preventing a person from voting as intended.
- Intentionally changing, attempting to change, or causing to be changed an official election document including ballots, tallies, and returns.
- Knowingly permitting, making, or attempting to make a false count of election returns.
- Intentionally concealing, withholding, or destroying election returns, or attempting to do so.

This paper will touch on, but not discuss in detail, areas such as voter registration fraud and multiple ballots from a single voter.

Electronic Voting Systems

First introduced in the 1970s, DRE voting devices capture votes electronically, without the use of paper ballots. Many election officials see electronic voting systems as a means for improving their ability to conduct and administer elections more efficiently. At the same time, many information technologists and activists have raised important concerns regarding the security of such systems. An important point is, however, that electronic voting systems have been introduced to make elections better (Celeste et al. 2005).

Fears about election rigging using electronic voting systems have animated critics for years, but there has been no conclusive evidence that such fraud has occurred (Barr 2006). Electronic voting systems have had technical problems – including unpredictable screen freezes – but technical glitches are not indicative of election fraud. And despite claims to the contrary, there are no documented cases of actual election tampering or hacking involving electronic voting machines (Merritt 2007; Wildermuth 2007). Electronic voting machines are not “computers.” Their programming does not compute or tabulate votes, it merely records any actions performed on the machine – in much the same way that a gas pump or ATM records actions performed on it. In addition, electronic voting machines have a single task – to record cast votes. They cannot multi-task as computers do. Most software firms deal with the inevitable bugs in their product by patching them; Microsoft still patches its seven-year-old Windows XP several times a month. But providers of electronic voting machines do not have this luxury, because any update must be federally tested for months (Thompson 2008).

Some people have equated electronic voting machines (particularly touch screen DRE voting devices) to check-in terminals at the airport, citing that “miscalibration somehow never seems to happen when you use the airport touchscreens [sic], hopping to ‘2’ bags when you press ‘1’ bag” (Harris 2007). However, the touch screens used for ATMs and baggage check-in are static; the touch sensors do not need to change periodically. In contrast, the sensors on a touch screen voting device must be re-calibrated for every election because the ballot is different each time.

The likely danger of touch screen machines is not from malice but from error. The perception or allegation of election fraud involving electronic voting systems is not an indication of actual fraud.

In 2002, Georgia was the first state to replace its old voting system with new DRE voting devices from Diebold Election Systems (now Premier Election Solutions). During the Georgia Senate race that fall, incumbent Democrat Max Cleland lost his bid for re-election. Freelance journalist Bev Harris suggested the results were suspect. The only evidence was that Cleland had been leading in the final pre-election poll by five points but wound up losing by seven points. However, there was no evidence of election fraud. Cleland himself says the campaign against him was dirty, but acknowledges that he lost fairly. He has stated that Georgia’s adoption of electronic voting was a good thing (Fund 2004).

In 2004, in Carteret County, North Carolina, a UniLect voting machine with a capacity of about 3,000 votes was used to record more than 7,000 votes, resulting in the loss of about 4,500 votes. As a result, a new election had to be held. Incidents of this kind usually can be traced to engineering failures: if the voting machine had been engineered not to accept ballots once its memory was full, the problem would not have occurred (Shamos 2007). However, the human factor cannot be ignored. Although there was apparently some confusion as to which model of voting machines was used, a UniLect official stated that the machines flash a warning message when there is no more room for storing ballots. It is possible that poll workers and election officials ignored or overlooked this warning (Associated Press 2004).

On November 7, 2006, an electoral disaster occurred in Sarasota County, Florida: Almost 18,000 people, about one in seven of the people who voted electronically, left the polls without recording a vote in the 13th U.S. Congressional District race, the hottest race on the ballot. Most observers agree that few of these voters deliberately skipped voting in that race—even on an electronic ballot that was 21 pages long followed by four pages of review screens. Instead, voters either overlooked that race due to the layout of the ballot, or the ES&S iVotronic touch screen voting machines somehow failed to record their votes (Jefferson 2007; Shamos 2007).

A considerable amount of technical investigation has been done into the circumstances of the Sarasota County election. The investigative team presented and tested three primary hypotheses for the cause of the problem (Jefferson 2007):

- Malicious code – The software in the voting machines might have contained logic that was deliberately designed in a way that would benefit a preferred candidate by not recording some votes. (If true, this would constitute election fraud.) The Florida Department of State performed parallel testing on a random sample of voting machines on Election Day. No unexplained anomalies were found, and hence there was no evidence of malicious code.
- Software bug – The software or hardware in the voting machines may have had a subtle bug of some kind that caused some votes to go unrecorded. The investigative team spent hundreds of hours manually reviewing the voting machines’ software code. In addition, the team performed automated static analysis and an extensive study of the problem symptoms and the execution environment. Extraordinary pains were taken to look for all conceivable problems in the source code, and none were found.
- Ballot layout – The layout of the ballot on the screen was misleading in a way that caused many voters to inadvertently skip the congressional race. In hindsight, the layout of the ballot looks especially problematic. On the iVotronic screen, there are no menus, icons, windows, or scrolling—just active areas that are not even surrounded by strong borders. The congressional race was sandwiched between two major statewide races, without the aid of a large, colored heading. The investigative team determined that voters trying to learn the interface, or voters who

are more visually than textually oriented were more likely to miss voting in the congressional race.

Ballot layout was determined to be the most likely explanation for the undervotes in the 2006 Sarasota County election. The choice of lettering size, horizontal and vertical lines, borders, shading, color, screen contrast, and overall layout should all be considered in designing a ballot that is easy to read and understand. It should also be remembered that even people who never miss an election only vote about once a year for about 10 minutes. From one election to the next, voters do not generally remember the layout used in a voting machine; they must relearn them each time (Jefferson 2007). This issue emphasizes the need for simple, easily understandable ballot layout.

In the summer of 2007, a top-to-bottom review of voting systems was conducted at the request of California Secretary of State Debra Bowen. The final report stated that the Sequoia, Diebold and Hart InterCivic voting systems were easily hacked by a team of computer experts commissioned to probe the machines for weaknesses. But election officials and voting machine providers alike rebutted claims made in the report. They stated that the performance of the review in a laboratory environment by computer security experts with unfettered access to the machines was unrealistic. In addition, the testing did not consider security procedures or real-world responses to potential hacking that jurisdictions typically put in place. The review was completed in five weeks, a time span that even Bowen's team of computer experts said was too brief to offer a complete understanding the systems' flaws (Harmon 2007). Only the Hart Voting System was subsequently re-approved, even conditionally, for use in the ensuing elections in the State of California.

Incidents have occurred in the use of electronic voting machines in the context of elections – errors or glitches – that have affected election outcomes. In test environments, under extreme conditions, technicians have breached voting equipment security. However, one problem that has never been encountered is a security incident involving an electronic voting machine in a live election. In the 28-year history of DRE voting machines, there is no evidence that anyone has ever breached security to alter the outcome of an election (Shamos 2007).

Paper Ballots

Using paper ballots does not automatically guarantee a secure election process. Voting with pencil and paper creates its own problems. Politicians have been stuffing ballot boxes since senators wore togas (Levitt and Waldman 2007). Ballot boxes can be lost or misplaced, to be found weeks after an election. In 2004, a worker at a Toledo, Ohio, election office found 300 completed absentee ballots in a storage room more than a month after the election. At least half hadn't been counted, and they affected the result of at least one local contest (Fund 2006). "If you look at the history of election fraud, you are really talking about paper," states Merle King, executive director of the Center of Election Systems at Kennesaw State University in Georgia (Merritt 2007).



Perhaps the most infamous case of ballot box tampering involves the way Lyndon Johnson's political career was saved in 1948 when he was losing a Democratic primary for U.S. Senate in Texas. A full week after the primary, an operative for political boss George Parr adjusted the vote total of Ballot Box 13 in Jim Wells County to include 200 additional votes for Johnson. That gave him an 87-vote victory statewide out of over a million votes cast. Interestingly, the voters of Box 13 apparently had cast their ballots in exact alphabetical order. Nevertheless, Johnson's victory survived every legal challenge and set him off on a career path that led to the White House (Fund 2004). More recent allegations of fraud in this part of Texas involve voter intimidation, voter registration irregularities, and the misuse of absentee ballots.

The 1996 school board election in District 8 in the southeast Bronx, New York, was tainted by election fraud and ballot tampering. Before the election, incumbent school board member Carol Trotta had announced that she would not seek re-election and did not file a nominating petition. Her supporters, however, pushed her to run as a write-in candidate. On Election Day, some voters complained that the ballots they received at the polls already had Trotta's name written in. The Special Commissioner of Investigation for the New York City School District discovered that poll workers in several locations had

written in Trotta's name prior to handing the ballots to voters. Although the investigation did not uncover direct wrongdoing by Trotta, her vote total included ballots that were fraudulently cast. The Special Commissioner sent his findings against individual poll workers to the Bronx District Attorney, who found insufficient evidence to bring criminal charges. In 1998 the U.S. Department of Justice proposed settling the case by letting Trotta run again for her seat in a special election to be held under carefully controlled conditions, including outside monitoring (Steinburg 1996; Stancik 1997; Hartocollis 1998). Carol Trotta lost the subsequent election.

The Florida 2000 presidential election is often cited as an extreme case of election fraud. However, the problem of "hanging chads" may have had more to do with the lower-quality paper on which the ballots were printed rather than any attempt to subjugate the vote or commit election fraud.



Concerns about election fraud would not go away if all voting was conducted by mail. Overall, absentee/by-mail voting is the most vulnerable to fraud. The potential for fraud is greatest in this area because of a lack of uniformly strong security measures in place in all states to prevent fraud (Minnite and Callahan 2003). In fact, most of the documented cases of voting fraud in the United States in recent years involve absentee ballots. Absentee voting makes it easier to commit election fraud because the ballots are cast outside the supervision of election officials.

The 1997 primary mayoral election in Miami, Florida, is perhaps the most notorious case of absentee ballot fraud in recent history. Running for re-election as mayor, Joe Carollo received 51 percent of the ballots cast at the polls, while his opponent, former

mayor Xavier Suarez, received 61 percent of the absentee ballots. Carollo challenged the election results, claiming fraud in the absentee ballot vote. At the subsequent trial, an expert documents examiner testified that 225 absentee ballots cast had forged signatures; there was evidence of 14 stolen ballots and 140 improperly witnessed ballots. Officials discovered that nearly 70 percent of the absentee ballots had been cast from the city's Little Havana district. One vote broker, 92-year-old Alberto Rossi, was found guilty of four counts of felony voter fraud – after investigators found at least 75 filled-out absentee ballots in his home, including the absentee ballot of a dead man. City Commissioner Humberto Hernandez, a political ally of Suarez, was also convicted of voter fraud. The trial judge concluded that "the evidence shows a pattern of fraudulent, intentional and criminal conduct that resulted in such an extensive abuse of the absentee ballot laws that it can fairly be said that the intent of these laws was totally frustrated.... This scheme to defraud, literally and figuratively stole the ballot from the hands of every honest voter in the city of Miami." The court ruled that Miami's new mayor was Joe Carollo, rather than Xavier Suarez. In 1998, the Florida state legislature passed a \$4 million election law reform package to expose future voter fraud (Fund 2004; Minnite and Callahan 2003).

Like electronic voting systems, paper ballots and ballot scanners have also been subjected to unrealistic testing. Paper ballots damaged with various household products were at least partially responsible for voting systems flunking recent re-certification testing by the Colorado Secretary of State's office. The damaged ballots were smeared with lipstick, blotted with mayonnaise, or clamped with a paper clip, among other abnormalities – as well as containing hesitation marks. "The certification process tests the equipment, but it doesn't test it in a real election situation, taking in the front-end processes and the back-end processes," states Hillary Hall, County Clerk of Boulder County, Colorado (Snider 2008). In a real-world election situation, election officials would look at the ballots before they were fed into the scanning devices. In addition, a random selection of ballots would be looked at after being scanned to make sure the ballots were counted correctly. In a properly administered election, the number of votes brought into question by problems with the paper ballot is likely to be well below one percent (Jones 2002).

Most paper ballots used in the United States are a form of Australian secret ballot, designed so that the ballot may be machine counted. This type of ballot was first used in 1858. Whether hand or machine counting is used, voters using an Australian ballot are instructed to vote using a prescribed mark written in the voting target. The target may be a square, oval, or broken arrow. The prescribed mark may be an X, blot filling in the oval, or a line connecting the two halves of the arrow. No technology based on machine-counted Australian secret ballots can eliminate all marginal marks. And with many voting systems, visual inspection by the voter is not sufficient to determine if the mark will or will not be detectable by the machine (Jones 2002).

Some activists have claimed that paper ballot voting and hand-counted election results work in other countries, so why not in the United States? Despite their use in foreign countries, hand-counted paper ballots are largely impractical in the United States. Our ballots are far more complicated than any other country's. For example, the 2006 (off-year) general ballot in Marin County, California, included 98 candidates in 30 races as well as 30 ballot propositions. The resulting mark-sense ballot was six pages long. With such long ballots it would take many days to calculate results. And the potential for election administrator error or fraud – if votes were really counted by hand, as opposed to scanned – would be enormous (Shamos 2007; Hasen 2006). In addition, elections in the United States include such complexities as vote-for-multiple candidates; fusion voting; straight-party voting; cross-over voting; candidate rotation; open, pick-a-party, and modified closed primary voting; fractional cumulative voting; and instant-runoff voting. Accurately hand-counting large numbers of paper ballots with these complex variations would be nearly impossible.

By contrast, most other countries use extremely simple ballots. In the more than 90 parliamentary and multi-party democracies in the world, voters typically select a party, rather than individual candidates. In other words, one race, one choice (Shamos 2007).

Since 2001, there have been at least 342 cases of electoral malpractice reported by the British police to the Crown Prosecution Service. One of England's most senior policemen has suggested that postal (by-mail) voting is wide open to corruption (Walker 2007). In Birmingham, England, six councilors were found guilty of corruption and a systematic attempt to

rig the 2004 city council elections. According to the proceedings, candidates and their supporters set out to steal, forge, and tamper with postal ballots in huge quantities (Merrick 2006). In 2006, the government began enacting new laws regarding postal ballots in an attempt to reduce the possibility of election fraud. The Electoral Commission also released a code of conduct for political parties, candidates, and canvassers on the handling of postal vote applications and postal ballots (White and Moulton 2008). The code's aim is to balance the importance of encouraging people to vote with the need to protect secrecy and minimize the risk or perception of fraud.



In 2007, Canadian Elections Commissioner William Corbett concluded two lengthy investigations into complaints from the last election involving allegations of wrongful voting in Edmonton Centre and northern Saskatchewan. Despite raging controversies at the time, investigators found no evidence of intentional fraud that affected the vote. However, committee members have proposed a bill requiring photo IDs for all voters to reduce the possibility of fraud in the polling place (Naumetz 2007).

Electronic vs. Paper

New voting technologies tend to emerge out of crises of confidence. We change systems only rarely, and then in response to a public anxiety that electoral results can no longer be trusted (Thompson 2008). "Historically, any voting jurisdiction is more likely to experience problems with new equipment," states Kimball Brace of Election Data Services, a nonpartisan consulting firm specializing in elections administration (Jennings 2006).

America voted on paper, until ballot-box stuffing and lost bags of ballots led many jurisdictions to abandon that system. Many jurisdictions subsequently adopted mechanical lever machines, but meaningful

recounts were impossible because the machines do not preserve each individual vote. Punch card systems then came into wide use, and these ballots could be stored for a recount. Punch cards worked for decades without controversy – until the 2000 presidential election and the infamous “butterfly ballot.” The Help America Vote Act of 2002 (HAVA) provided incentives for jurisdictions to replace their punch card and lever machines. Electronic voting machines seemed like the perfect answer to the hanging chad. Not only were votes stored in digital memory, but they could be preserved in several locations within the voting system. In addition, the technology allowed persons with disabilities to vote unassisted, often for the first time.



From the beginning, the new machines have touched off a firestorm of controversy and a wide range of opinions. Election officials cite that electronic voting systems give them tabulated election results much more quickly, sparing them long hours on Election Night. Computer experts say the machines could be hacked into, despite the fact that there is no evidence of someone successfully hacking an electronic voting machine. Critics claim the devices cannot be trusted and urge a return to paper ballots.

To address the public’s concerns about electronic voting systems, many jurisdictions are turning to optically scanning paper ballots. Optical scan voting systems use electronic technology to tabulate paper ballots. Although optical scan technology has been in use for decades for such tasks at scoring standardized tests, it was not applied to voting until the 1980s (U.S. Government Accountability Office 2005).

However, optical scanning is hardly a flawless system. If someone doesn’t mark a ballot clearly, a recount can become an argument over “voter intent.” The machines often need to be calibrated so they don’t miscount ballots. Poorly trained poll workers could lose ballots. And the machines do, in fact, run software that can be hacked. There are also serious

logistical problems for jurisdictions that are switching to optical scan machines during an election year. Experts estimate that it takes at least two years to retrain poll workers and employees on a new system (Thompson 2008). In addition, voters have complained that filling out a paper ballot takes longer than using an electronic voting device. Persons with disabilities and the elderly often have difficulty reading paper ballots due to the font size used.

Often during discussions of the merits of electronic voting systems vs. paper-based systems an important distinction between document ballots and non-document ballots is lost or ignored. Document ballots are those marked by a voter on a physical medium. Non-document ballots are those where the totals are recorded on counters or ballot images are stored electronically (Shamos 2007).

A document ballot, such as an optical scan ballot, provides only one copy, namely the one marked by the voter, and this copy must be handled to be tabulated. In the handling, a document ballot may be altered or substituted, and once a substitution is made, it is impossible to recover the original voter’s selections, which are gone forever. The movement from paper to lever machines to DRE voting devices was an effort to eliminate the inherent insecurity of document ballots (Shamos 2007).

By contrast, in a DRE system multiple copies of ballots are retained on different media in different physical locations. To affect the outcome of an election, redundant encrypted records would have to be altered. To date, no one has even suggested, let alone demonstrated, a way to do this (Shamos 2007). A 2006 report by the Brennan Center for Justice explored the possibility of election tampering as it pertained to electronic voting systems and precinct-based optical scan (paper ballot) systems (Norden 2006). According to the study, any voting system is vulnerable to a concerted attack by persons trying to subvert an election. All the election tampering scenarios reviewed would require a number of co-conspirators (from just a few to over a hundred) to have any possibility of success. Some scenarios required that members of the elections office staff be involved in the tampering conspiracy, and doing so means that those election officials would be willing to commit felony crimes and possibly face prison time. However, the most troubling vulnerabilities of each system can be substantially remedied if proper countermeasures are implemented at the state and local levels.

ELECTION SECURITY AND BEST PRACTICES

The perception persists that we cannot control the security of isolated voting machines that are not connected to the Internet, but that problems with the production, storage, transportation, and counting of paper ballots were solved long ago (Shamos 2007).

“The main flaws are not in the software, hardware, or in the data transmission systems, but in the human links that control the connections,” states Antonio Dourado de Rezende, a computer science professor at the University of Brasilia (Lehman 2006). Voting system security is a combination of people, procedures, and technology. *Any voting system, even an all-paper, hand-counted system, is going to face similar security needs.*



Security

Some basic security guidelines were presented in the Brennan Center’s study (Norden 2006):

- Conduct automatic routine audits
- Perform parallel testing on Election Day by selecting voting machines at random and testing them as realistically as possible
- Ban the use of voting machines with wireless connections
- Use a transparent and random selection process for all auditing procedures
- Ensure decentralized programming and voting system administration by allowing jurisdictions to choose their own voting system and providing the ability to conduct elections that are independent of the voting system provider
- Institute clear and effective procedures for addressing evidence of fraud or error.

Best Practices

Dana DeBeauvoir, the County Clerk of Travis County, Texas, provides additional detail to these guidelines with some best practices drawn from her

own experience in conducting elections (DeBeauvoir 2005):

- Provide public invitation to attend all programming and testing activities
- Maintain written procedures and initialed tracking sheets
- Maintain independence from voting system providers
- Recruit, screen, and train skilled and trusted employees
- Use law enforcement officers to secure early voting ballot boxes
- Improve security for the building where election activities occur
- Implement employee procedures that lower risk
- Conduct extensive pre-purchase testing of new equipment or software
- Provide continuous functionality testing of equipment
- Conduct hash code testing on software
- Perform high-volume testing of ballot programming
- Perform parallel testing during Early Voting and on Election Day
- Conduct Early Voting and Election Day audits by matching counts of voters by location as reported by the electronic voting system to the number of names on signature rosters
- Conduct post-election verification using the three redundant electronic sources, paper results printed from the electronic ballot boxes, and precinct-by-precinct election results. A voter verifiable paper audit trail (VVPAT) can also be used in the post-election verification process, if allowed by the jurisdiction.

In addition, DeBeauvoir insists that Travis County generate and produce its own ballots rather than relying on the County’s voting system provider. The Travis County election system generally gets good marks, even from the harshest critics of electronic voting, because of the attention to security (Copelin 2006). Security begins with low-tech solutions such as locks on doors, video cameras in secure areas, and limiting access to sensitive areas and equipment.

If sufficient safeguards are in place, absentee/by-mail ballot fraud can be greatly reduced. The State of Oregon maintains a vigorous signature-matching process for qualifying mail-in ballots. Approximately 2½ weeks before Election Day, local registrars mail

ballots, and instructions for returning them, to all registered voters in their jurisdiction. Teams of election workers verify the signature on each returned ballot against computerized records of registered voters. Any ballots whose signatures do not match are turned over to the county election clerk for investigation, which may include contacting the voter. If fraud is suspected, the clerk forwards the case to the Secretary of State's office, which then forwards cases to the Attorney General for prosecution. From 1993 to 2003, 1,001 cases of multiple voting and 1,056 cases of signature-matching problems have been referred to the Secretary of State's office for investigation – out of tens of millions of votes cast. Only 15 of these cases were referred to the Oregon Attorney General for possible prosecution. In at least six of the cases, people were found guilty of voter fraud, contaminating approximately 12 ballots (Minnite and Callahan 2003).

Barcode numbering of absentee/by-mail ballots offers an additional level of security. Duplicate or fraudulent returned ballots can be more easily detected.

CONCLUSION

Voting in the United States has always been subject to manipulation. Since the earliest days of paper ballots, a wide variety of techniques have been used to influence election results. These techniques include forging, altering, destroying, substituting, and augmenting ballots, to say nothing of vote buying and other coercive schemes (Shamos 2007).

Scare stories regarding election fraud with electronic voting systems abound on the Internet and on editorial pages, quickly becoming accepted wisdom. The stories take on the character of urban legend. However, the notion of widespread election fraud in the United States is itself a myth. A demonstration that an attacker, under unrealistic conditions, might corrupt an electronic voting machine – although a cause for concern – does not justify discarding an entire technology (Shamos 2007).

Studies show that election fraud of any kind is not widespread. A statewide survey of Ohio's 88 county boards of elections found only four instances of ineligible persons attempting to vote out of a total of 9,078,728 votes cast in the state's 2002 and 2004 general elections. This is a fraud rate of 0.00000045 percent. The 2005 report from the

Commission on Federal Election Reform (known as the Carter-Baker Commission) noted that since October 2002, federal officials had charged 89 individuals with casting multiple votes, providing false information about their felon status, buying votes, submitting false voter registration information, and voting improperly as a non-citizen. Examined in the context of the 196,139,871 ballots cast between October 2002 and August 2005, this represents a fraud rate of 0.0000005 percent (Serebrov and Wang 2006).

The good news is that election systems, and elections themselves, are improving. The harsh light that illuminated the flaws in the 2000 national election led to academic research, provoked legislative action, spurred innovation in the marketplace, and educated the public about the strengths and weaknesses of elections in the United States (Alvarez and Antonsson 2007). Steadily improving voting technology has also served to reduce opportunities for election fraud. As a whole, U.S. voting systems are substantially more reliable and ensure higher levels of voting integrity than was the case even a few decades ago (Minnite and Callahan 2003). Improving our voting systems is an evolutionary process, not a revolutionary one.

The actual extent of election fraud will always be in dispute. Not only can investigative findings be misleading as to the extent of fraud, but they can also dramatically overstate the actual impact on elections (Harvard Law Review 2006).

In the end, there is no smoking gun of election fraud – the deliberate corruption of the process of casting and counting votes – with regard to electronic voting systems. More often than not, it is people – whether it is insufficient training, a shortage of workers, or human error – at the root of problems associated with elections. By using good security procedures and best election management practices, election officials can continue to protect against election fraud and ensure fair and accurate elections within their jurisdictions.

"No election system is ever good enough for the candidate who loses the election." John Lindback, Director of the Elections Division for the Oregon Secretary of State

References

- Alvarez, R. Michael, and Erik K. Antonsson. "Bridging Science, Technology, and Politics in Election Systems." *The Bridge*. National Academy of Engineering. Vol. 37, No. 2. Summer 2007.
- Ascribe Newswire. "Study: Touch Screen Voting a Hit; Critics Miss Mark on Security." January 22, 2008.
- Associated Press. "More than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity." *USA Today*. November 4, 2004
- Barr, Cameron W. "Security of Electronic Voting is Condemned." *Washington Post*, December 1, 2006.
- Celeste, Richard, Dick Thornburgh, and Herbert Lin, editors. *Asking the Right Questions About Electronic Voting*. The National Academies Press. 2005.
- Copelin, Laylin. "In High-Tech Age of E-voting, Snags Usually Low-Tech." *Austin (Texas) American-Statesman*. June 13, 2006.
- DeBeauvoir, Dana. "Method for Developing Security Procedures in a DRE Environment." *Professional Practices Papers*, proceedings of the Election Center 21st Annual National Conference. 2005.
- Donsanto, Craig C. "Prosecution of Electoral Fraud under United States Federal Law." *IFES Political White Paper Series*. IFES. 2006.
- Follman, Mark, Alex Koppelman, and Jonathan Vanian. "How U.S. Attorneys Were Used to Spread Voter-Fraud Fears." *Salon.com*. March 21, 2007.
- Fund, John. *Stealing Elections: How Voter Fraud Threatens Our Democracy*. Encounter Books. 2004.
- Fund, John. "Absent Without Leave." *The Wall Street Journal*. October 30, 2006.
- Harmon, Steven. "E-Voting Vendors: Any Machine Can Be Hacked in a Lab." *Shakey Ground* (newsletter of the Colorado Rocky Mountain Chapter of the Association of Contingency Planners). August 2007.
- Harris, Bev. www.BlackBoxVoting.org. Post Number: 7069. November 12, 2007.
- Hartocollis, Anemona. "School Vote in the Bronx is Proposed." *The New York Times*. January 7, 1998. *Harvard Law Review*. Vol. 119:1127. pages 1144-1154. "III. Voter Identification Laws." February 2006.
- Hasen, Richard L. "Keeping the Voting Clean." *The New York Times*. November 11, 2006.
- Jefferson, David. "What Happened in Sarasota County?" *The Bridge*. National Academy of Engineering. Vol. 37, No. 2. Summer 2007.
- Jennings, Trip. "Ballots Switch to Paper; Results in Change Mixed." *Albuquerque (New Mexico) Journal*. October 19, 2006.
- Jones, Douglas W. "Counting Mark-Sense Ballots: Relating Technology, the Law and Common Sense." University of Iowa. Voting and Elections web pages. 2002.
- Lehman, Stan. "Electronic Voting Raises New Election Questions in Brazil." Associated Press. September 29, 2006.
- Levitt, Justin, and Michael Waldman. "The Myth of Voter Fraud." *People's Weekly World*. April 7-13, 2007.
- Merrick, Rob. "Merseyside to Test Plan to Stamp Out Voter Fraud." *Daily Post* (Liverpool, England). February 14, 2006.
- Merritt, George. "Electronic Voting is Questioned." Associated Press. December 31, 2007.

- Minnite, Lori, and David Callahan. *Securing the Vote: An Analysis of Election Fraud*. Dēmos: A Network for Ideas and Action. 2003.
- Nather, David. "Election Board Facing Votes of No Confidence." *Congressional Quarterly Weekly*. April 24, 2007.
- Norden, Lawrence, lead author. *The Machinery of Democracy: Protecting Elections in an Electronic World*. Brennan Center for Justice at NYU School of Law. 2006.
- Naumetz, Tim. "Elections Watchdog Praises 'Lawfulness' of Canadian Voters." *Ottawa (Canada) Citizen*. February 9, 2007.
- Serebrov, Job, and Tova Wang. *Voting Fraud and Voter Intimidation: Report to the U.S. Election Assistance Commission on Preliminary Research & Recommendations – Draft*. 2006.
- Shamos, Michael Ian. "Voting as an Engineering Problem." *The Bridge*. National Academy of Engineering. Vol. 37, No. 2. Summer 2007.
- Snider, Laura. "Mayo Foils Voting Machines." Boulder (Colorado) Daily Camera.
- Stancik, Edward F. *Filling in the Blanks: An Investigation into the Write-In Votes for Carol Trotta in Community School District 8*. City of New York, The Special Commissioner of Investigation for the New York City School District. April 1997.
- Steinburg, Jacques. "Ballot-Fraud Investigation." *The New York Times*. May 24, 1996.
- Thompson, Clive. "Can You Count on These Machines?" *The New York Times*. January 6, 2008.
- U.S. Election Assistance Commission. *Election Crimes: An Initial Review and Recommendations for Future Study*. December 2006.
- U.S. Government Accountability Office. *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*. Report GAO-05-956. September 2005.
- Walker, Kirsty. "Dump E-voting to Stop Fraud, Labour Warned." *Daily Mail* (London, England). February 28, 2007.
- White, Isobel, and Mo Moulton. *Postal Voting and Electoral Fraud*. Standard Note SN/PC/03667. Parliament and Constitution Centre, House of Commons. January 23, 2008.
- Whitehead, John W. "Voter ID Laws Threaten Our Freedom." *The Times of Trenton* (New Jersey). January 16, 2008.
- Wildermuth, John. "Secretary of State Doubtful of Electronic Voting's Future." *The San Francisco Chronicle*. December 2, 2007.