Stop the Presses: How Paper Trails Fail to Secure e-Voting

BY DANIEL CASTRO[1] | SEPTEMBER, 2007

A federal mandate to require voter-verified paper audit trails for all electronic voting machines would prevent the use of innovative voting technology that offers more security, transparency, and reliability than paper-based audit trails alone.

Americans trust computers to run critical applications in fields such as banking, medicine, and aviation, but a growing technophobic movement believes that no computer can be trusted for electronic voting. Members of this movement claim that in order to have secure elections, Americans must revert to paper ballots. Such claims are not only incorrect but attack the very foundation of our digital society, which is based on the knowledge that information can be reasonably secured. Clearly, no system with a human element—including electronic and non-electronic voting machines—is error-proof, and specific versions of certain voting machines have security weaknesses. Neither of these facts, however, should be taken as a universal indictment of e-voting.

Direct recording electronic (DRE) voting machines are electronic machines, similar to ATMs, that let voters view ballots on a screen and make choices using an input device such as buttons or a touchscreen. Some opponents of electronic voting are lobbying for legislation that would require so-called "voter-verified paper audit trails" for all DRE voting machines. The purpose of the paper audit trails would be to provide proof that the DRE voting machines functioned correctly. Unfortunately, as discussed in this report, paper audit trails for DRE voting machines have several shortcomings. They do not provide complete security to voters and they increase costs and risks. Furthermore, requiring voter-verified paper audit trails would prevent the use of innovative voting technology that offers voters more security, transparency, and reliability than can be delivered with paper audit trails alone.

Congress is now considering legislation that would mandate that all DRE voting machines have voter-verified paper audit trails, and many states will vote on similar legislation this year. We believe it is time for the debate on e-voting technology to move beyond a discussion of

paper audit trails. To restore voter confidence and promote secure election technology in the United States by ensuring that states can continue to improve their voting systems, we recommend the following:

- Congress and the states should allow the use of fully electronic ballots, not restrict electronic voting systems to those that create paper ballots.
- Congress and the states should require that future voting machines have verifiable audit trails, not require machines that create verifiable paper audit trails.
- Congress should provide funding for the U.S. Election Assistance Commission to issue grants for developing secure cryptographic voting protocols and for pilot testing of new voting technology.

ELECTIONS IN THE UNITED STATES

Voting machines used in U.S. elections must satisfy many requirements. First, virtually every state requires a secret (or Australian) ballot, so the machines must allow secret ballots. In the late 1800s, election officials in the United States introduced the secret ballot as an improvement to voice votes and party tickets.[2] A secret ballot has the following properties: it must contain the names of all candidates and the text of all propositions; it must be distributed only at the polls; and it must be marked in secret.[3] Maintaining the confidentiality of voters' selections helps election officials limit voter coercion and vote selling. Second, elections must be secure, so the integrity of the voting machines and ballots must be maintained at all times, and voters must be permitted to vote only once and only in the elections in which they are eligible. Third, elections must be auditable so that election officials can verify that the results of the election are accurate.[4]

One difficulty with administering secure and confidential elections in the United States is that there is no trusted third party. A trusted third party is an entity that facilitates transactions between two entities. If the two entities trust a third party, they can use this trust to secure their own interactions. Thus, for example, a notary public provides third-party verification for authenticating and verifying a signature. In theory, election administrators are trusted third parties; in fact, however, many of these individuals are either elected officials or political appointees, so they have a conflict of interest. In the 1920s, one of the primary reasons for moving from paper ballots to mechanized voting was to eliminate the reliance on human participants.[5]

The integrity of a paper ballot still depends on physical security controls. Historically, failed security controls have led to modified, spoiled, and stolen ballots, as well as to stuffed ballot boxes.

Voting machines used in U.S. elections must also adhere to a number of usability requirements. First, a number of federal laws, including the Americans with Disabilities Act, the Voting Rights Act of 1965 (as amended in 1982), the Voting Accessibility for the Elderly and Handicapped Act of 1984, and the Help America Vote Act of 2002, guarantee the right of disabled individuals to participate in elections. Second, in many precincts, election material must be available in multiple languages.[6] Third, many states require that voters be allowed to include write-in votes. Fourth, states are required to allow a voter to cast a provisional ballot even if the voter appears to be ineligible to vote. Fifth, some states require ballot rotation so that a candidate cannot gain an advantage from the placement of his or her name on the ballot. Finally, some elections use preferential voting, where voters rank their chosen candidates to avoid the need for a runoff election.

THE PROBLEM WITH PAPER BALLOTS

Voting technology has evolved and improved over time as a result of several technical advances. Before the mechanization of the industrial revolution, voters relied on paper ballots. In the early 1900s, election officials overwhelmingly decided to use mechanical voting machines after witnessing years of fraud and error with paper ballots.[7] Advertisements proclaimed that mechanical lever machines were completely secure because they did not rely on humans to hand count each vote. When voters pulled the lever, their vote was immediately cast and tallied. Voters no longer had to wonder if their ballot would be lost, misinterpreted, or considered a spoiled ballot.[8]

In the late 1950s, as mainframe computers were developed, computerized vote processing was introduced as a more efficient means of vote tallying. By 1982, more than half of the American electorate was using punch-card voting machines, which had replaced lever machines as the dominant voting technology. These machines used the punch-card paper ballots made infamous during the controversial 2000 U.S. presidential election.[9]

As history has repeatedly shown, traditional paper ballots are not a secure form of voting. Although some current legislation calls for "durable paper ballots," the term durable is misleading because such ballots are required to withstand only basic handling.[10] The integrity of a paper ballot still depends on physical security controls. Historically, failed security controls have led to modified, spoiled, and stolen ballots, as well as to stuffed ballot boxes. The story of how Lyndon B. Johnson used paper ballots to commit fraud demonstrates the weaknesses of paper ballots.

Another problem with paper ballots is that voters may add extraneous marks to identify their ballot to a third party. If their ballot can be identified by a third party, such as an election official, then voters can engage in vote selling. A common countermeasure to this tactic is to consider any ballot with extraneous marks as a spoiled ballot. The downside to this countermeasure is that it is easy for election officials to spoil a ballot, especially during a manual recount.

BOX 1: HOW LBJ USED PAPER BALLOTS TO STEAL AN ELECTION[11]

The story of Lyndon Johnson's election in 1948 to the U.S. Senate illustrates how paper ballots enabled fraud and corruption in American elections. Johnson first ran for the U.S. Senate in 1941, when Texas held a special election to fill the seat of a recently deceased senator. Johnson was a 32-year-old congressman at the time, and many thought he would soon become the youngest senator in the country. As Election Day approached, all of the polls showed Johnson in the lead against his opponent Governor Pappy O'Daniel.

Confident that he would win, Johnson told the precinct bosses he controlled that they could report their results immediately. This decision proved to be a critical mistake. Conventional wisdom at the time said that candidates should always wait until the last minute to report the totals in the precincts they controlled. This prevented their opponents from learning how many votes they needed to add to win the election. When Johnson allowed his men to call in their totals early, he gave O'Daniel all the advantage he needed. While Johnson celebrated what he thought was a certain victory, O'Daniel's campaign quickly had their own men add more votes to their tallies.

The next day Johnson was shocked when he discovered that he had lost the first election of his life. He would not forget this defeat or the means by which he lost. Seven years later, in his second run for the Senate, Johnson faced the popular former governor Coke Stevenson in the Texas Democratic state primary. Johnson waged an aggressive and expensive campaign against his opponent, but Stevenson won a plurality and beat Johnson by 70,000 votes. He did not win a majority, so a runoff election was scheduled.

Although Johnson slowly narrowed the gap in the polls between Stevenson and himself, as the runoff election date grew closer, Johnson's campaign aides realized Stevenson still maintained a solid lead. Unable to obtain the remaining votes through conventional methods, Johnson's campaign directed their funds to the political machines that controlled the minority voting blocs along the border and in San Antonio. These investments paid off. For example, in the notoriously corrupt Duval County controlled by George B. Parr, not only did Johnson receive an overwhelming 99 percent of the vote, but the county recorded a 99.6 percent turnout of all registered voters, a record level of civic participation. Unfortunately for Johnson, on election night, Stevenson still led by 854 votes.

Stevenson would not remain in the lead for long. Johnson and his campaign aides worked the phones over the next few days to persuade local leaders to "find" a few more votes for Johnson. In many counties this was impossible. In

(continued)

VOTING MACHINE REFORM AFTER THE 2000 PRESIDENTIAL ELECTION

After the controversial 2000 U.S. presidential election, many voters decried the inaccurate and inconsistent voting systems used throughout the country and demanded change. Congress responded with the Help America Vote Act (HAVA) of 2002, which was intended to help states modernize their aging electromechanical voting systems.[13] HAVA includes the following provisions:

- establish the U.S. Election Assistance Commission (EAC), an independent federal agency tasked with creating voluntary voting system guidelines and minimum election administration standards for states and local government
- provide nearly $4 billion in funding for states to replace their lever and punch-card voting machines with more modern and more accessible voting systems[14]
- require states to implement a single, uniform, statewide, computerized voter registration database
- mandate that in the event a voter appears to be ineligible to vote, the voter may still cast a provisional ballot if he or she believes this ineligibility to be a mistake
- mandate that voters who register to vote by mail or who have never voted before in a federal election must provide either photo identification or other documented proof of their name and address

BOX 1 *(continued)*

San Antonio, Johnson had been able to buy almost 10,000 votes, but since the city voted by machine, once the mechanical tallies were certified, additional votes could not be added. Over the next few days, as precincts checked their votes, however, the tally slowly changed, and Stevenson's lead dropped to a handful of votes. Finally, around noon on the sixth day after the election, the Democratic Executive Committee of Jim Wells County called the Election Bureau to report an amended return. The south Texas county, under the domain of the Parr political machine, claimed that they had misreported the figure for Johnson as 765 votes when the correct total was 965 votes. After all the dust settled, Johnson had won the election by a margin of 87 votes.

Vote buying had long been a part of Texas politics, but Stevenson declared that these additional 200 votes represented "the first time that the manipulators of the voting in these counties were not content with all-out bloc voting, but re-opened the boxes in secret long after the election had closed and stuffed them with a directed number of ballots."[12] Furious at the audacity of Johnson's vote stealing, Stevenson decided to prove his allegations of ballot stuffing and headed to Alice, the county seat of Jim Wells County, with Frank Hamer, the legendary Texas Ranger best known for tracking down and killing Bonnie and Clyde.

With the most feared lawman in the Lone Star State at his side, Stevenson marched past George Parr's armed gunmen and demanded to see the poll list held in the safe of the Texas State Bank of Alice. The poll list contained the names of every voter as they signed in to vote. Here Stevenson found the evidence he was seeking: the last 200 names on the poll list been added in a different color ink, in a single handwriting and in alphabetical order.

His lawyers spent the next weeks rounding up these voters who later testified under oath in federal court that they had not voted in the election. Armed with this evidence, along with evidence of voter fraud throughout the state, Stevenson tried desperately to block the state from certifying Johnson as the Democratic Party's nominee. He eventually took the dispute all the way to the U.S. Supreme Court, but after all copies of the poll list disappeared, the federal court ruled it did not have jurisdiction.

In the end, Johnson prevailed and eventually headed to the U.S. Senate with the sobriquet "Landslide Lyndon."

Although HAVA provided nearly $4 billion in funding for states to upgrade their voting systems, it did not mandate that the states use a specific voting technology. States could choose any voting technology, including DRE, optical scan, and lever voting machines, that met certain specified functional requirements (e.g., voting machines must be accessible for individuals with disabilities and have an audit capacity).

HAVA also mandated that EAC provide grants for pilot programs to test new technology in voting systems and grants for research and development "to improve the quality, reliability, accuracy, accessibility, affordability, and security of voting equipment, election systems, and voting technology."[15] HAVA authorized EAC to provide $10 million for pilot programs and $20 million for improving voting technology. Since 2002, Congress has failed to appropriate the $30 million to fund these grants authorized by HAVA.[16] Recently proposed legislation would provide approximately $1 billion in additional funding for states to procure new DRE voting machines with printers but would not first appropriate funds to develop and pilot test new voting technology. This legislation, if adopted, would force many states to discard their existing equipment if their current DRE voting machines cannot be upgraded to include a printer.

HAVA authorized EAC to provide $10 million for pilot programs and $20 million for improving voting technology. Since 2002, Congress has failed to appropriate the $30 million to fund these grants authorized by HAVA.[16]

Many of the reforms introduced by HAVA have strengthened the U.S. election system. The provisional ballot requirement has helped prevent many citizens from being denied the right to vote at the polls. In the 2004 elections, for example, 1.9 million voters nationwide cast provisional ballots; approximately 1.2 million (64.5 percent) of those provisional ballots were counted.[17] In addition, HAVA has increased the integrity of our elections by strengthening statewide voter registration databases.

HAVA authorized EAC to develop a national program to accredit voting system testing laboratories and national standards to test the voting systems. In 2005, EAC adopted the Voluntary Voting System Guidelines for states on voting equipment and election technologies. These guidelines, which will become effective in December 2007, provide "a set of specifications and requirements against which voting systems can be tested to determine if the systems provide all the basic functionality, accessibility, and security capabilities required of these systems."[18]

HAVA's requirements have helped speed the adoption of electronic voting machines as replacements for lever and punch-card voting machines. In 2000, just 10 percent of the counties in the United States (containing 13 percent of registered voters) used DRE voting machines, while 41 percent of counties (containing 29 percent of registered voters) used optical scan ballots.[19] In 2006, 36 percent of the counties in the United States (containing 38 percent of registered voters) used DRE voting machines,[20] and 56 percent (containing 49 percent of registered voters) used optical scan ballots.[21]

BENEFITS OF E-VOTING

Digital electronic voting solves a number of voting problems associated with electromechanical voting technology. In the 2000 U.S. presidential election, for example, punch-card voting machines created ballots with half-punched ballots. When election officials could not determine voter intent, they had to discard these ballots. DRE voting machines eliminate this problem, because in the binary world of computers, "dimpled chads" do not exist. In addition, when completing a paper ballot, voters can easily mistakenly overvote or undervote and render their ballot invalid. DRE voting machines help eliminate these problems by preventing voters from casting invalid ballots, thereby ensuring that more ballots count.

Electronic voting also has the potential to revolutionize the voting process for blind, disabled, or illiterate voters. With paper ballots, many of these voters could vote only with the assistance of poll workers, which compromised both the confidentiality and the integrity of their ballots. Audio-based electronic voting

machines enable blind and illiterate voters to vote privately and independently. DRE voting machines also can have more user-friendly interfaces to make voting simpler. For example, DRE voting machines can show voters a summary of their ballot, allowing them easily to verify that they have not made an error.

Finally, many states allow early voting at central polling locations throughout the state in the days prior to Election Day. Early voting helps make voting more accessible to people who might otherwise be unable to vote on the day of the election. Early voting with paper ballots is impractical and expensive because custom ballots must be made available for each precinct, often in multiple languages. Thus, for example, in Riverside County, California, election officials switched to DRE voting machines after they discovered that they wasted over half a million dollars in unused paper ballots in one election because of low voter turnout.[22] DRE voting machines can host ballots for every precinct, so election officials can more easily provide early voting. In addition, many DRE voting machines enable multilingual and non-English speaking voters to vote using their preferred language.

OPPOSITION TO DRE VOTING MACHINES

Unfortunately, the effort to bring voting machines into the digital age has been politicized by various interest groups, including BlackBoxVoting.org and VerifiedVoting.org. These groups have waged a full-scale assault on DRE voting machines. They decry the technology as inherently insecure while refusing any solution other than a return to paper ballots.

The success of these groups reflects the high degree of polarization and distrust in politics, as well as the emotional investment many people have in elections. Many opponents of electronic voting machines are motivated by a distrust of technology, anger at election results, and conspiracy theories about voting companies. For example, political strategist Bob Shrum has blamed Senator John Kerry's loss in 2004 on the electronic voting machines in Ohio and suggested that election officials intentionally rigged these devices to favor President Bush.[23] Opponents of fully electronic voting machines also rely on the fact that few Americans understand the technology behind electronic voting, such as cryptography. They scare voters and election officials into demanding something they do understand: paper.

Not surprisingly, some opponents of electronic voting machines have waged their battles in the courts. In Maryland, for instance, Linda Schade, the founder of TrueVoteMD, sued the Maryland State Board of Elections to force the board to decertify the Diebold voting machines and obtain an injunction to force Maryland to use paper ballots in the 2004 election.[24] The courts dismissed her motion and arguments and stated that although no election system could meet a standard of "perfect security," the court was "confident the votes of the Plaintiffs will be counted."[25]

Opponents of fully electronic voting machines also rely on the fact that few Americans understand the technology behind electronic voting, such as cryptography.

The debate on electronic voting was further politicized when Walden O'Dell, the CEO of Diebold, one of the primary manufacturers of e-voting equipment, was found to be a major fundraiser for the Bush re-election campaign in 2004. In addition, O'Dell distributed a fundraising letter in which he stated his commitment "to helping Ohio deliver its electoral votes to the president next year."[26] Since then Diebold, originally known for making ATMs, has been targeted by critics of e-voting for its allegedly insecure voting equipment. Initiatives such as "Hack the Vote" were created, and a monetary prize was offered to anybody who could prove that they could hack into an e-voting system undetected.[27] To date, nobody has claimed the prize money.

At the heart of the argument against e-voting is the notion that a computer cannot be trusted—an idea that flies in the face of our digital culture. In areas from online banking, to health information technology, to aviation, Americans trust computers every day with their lives and livelihood, not because computers are infallible, but because the benefits of technology significantly outweigh the risks. With any voting system

there is a margin of error, from either fraud or error, but e-voting offers the chance to minimize the margin of error by offering complete end-to-end auditing. The claim that "e-voting systems actually provide less accountability, poorer reliability, and greater opportunity for fraud"[28] is false and indefensible. Furthermore, as we discuss later in this report, some e-voting techniques use advanced cryptography that offer voters and election observers an unprecedented level of verifiability not achievable in traditional paper-based voting systems.

Demands for Voter-Verified Paper Audit Trails

Critics of electronic voting have demanded states add "voter-verified paper audit trails" to all DRE voting machines. If this approach were adopted, a DRE voting machine would print a paper ballot after each voter cast his or her electronic ballot. The individual voter could then verify that the printed paper ballot was correct. Depending on the system, the voter would either manually deposit this paper ballot into a ballot box or the voting machine would mechanically store the paper ballot. Advocates of adding voter-verified paper audit trails to all DRE voting machines have dubbed this approach "verified voting," because the voter can verify that the voting machine has created an audit trail of his or her vote.

Unfortunately, paper-based auditing trails such as these do not allow the voter to verify that the results of an election are accurate. A DRE voting machine can provide up to three different guarantees to a voter: first, that the vote was cast as intended; second, that the vote was recorded as cast; and third, that the vote was tallied as recorded.[29] The first property, that the vote was cast as intended, simply means that the DRE voting machine understood the voter intent. Such verification is typically provided to the voter when the DRE voting machine shows the voter's selection on the screen. The second property, that the vote was recorded as cast, means that the DRE voting machine recorded the correct vote for the voter. Paper audit trails are but one way to verify this property. The third property, that the vote was tallied as recorded, is not provided by voter-verified paper audit trails. Without this property, the other two guarantees are of less value. Ultimately, voters want to know that their vote was included in the final tally. Paper audit trails do not provide this assurance.

One of the most common arguments used by opponents of e-voting is that the DRE voting machine is essentially a "black box," and its operations are hidden from the voter. For most DRE voting machines, this statement is true. Historically, though, many types of voting machines, including the lever machines that were used for more than 100 years in U.S. elections, have been black boxes whose internal workings have been hidden from voters. There are always some people who mistrust new technology. In the 1960s, for example, people objected to using IBM computers to count punch-card ballots because of fears that the machines might switch votes.[30]

Contrary to the claims of e-voting opponents, though, merely adding paper audit trails to DRE voting machines does not make elections more secure. The problem is not "black box voting" but "black box elections." Most of the operations of the election, such as ballot collecting, ballot transferring, and ballot tallying are hidden from the voter. The result is that no voter, regardless of the presence or absence of paper audit trails, currently knows whether his or her vote was actually counted.

Ultimately, voters want to know that their vote was included in the final tally. Paper audit trails do not provide this assurance.

Another common argument made by opponents of e-voting is that without paper receipts, an attacker can easily make a voting machine alter ballots without being detected. [31] Opponents of e-voting use fear of the unknown and widespread ignorance about information security to create the illusion that DRE voting machines can easily be hacked. Unfortunately, this argument confuses two issues: attacking a computer versus attacking an election. As we explain later, most voting systems used today rely on both physical security and auditing to prevent election fraud. Opponents of e-voting such as BlackBoxVoting.org claim that they can "hack an election," but none of their attacks are plausible under real-world election scenarios, particularly

when the voting machines are correctly designed and implemented.[32] Unfortunately, claims that it is possible to "hack an election" are difficult for the average person or elected official to judge, because few Americans are information security experts.

For example, in July 2007, a group commissioned by the California secretary of state to review the state's voting machines released a report documenting the security vulnerabilities that they found. [33] The report received much press, and critics of e-voting pointed to this report as proof that DRE voting machines can be hacked. While the report serves as a valuable tool to evaluate and improve the security of these machines, the so-called "attacks" detailed in the report are inconsequential. While these attacks may work in the lab, most of these attacks are unrealistic in real-world election conditions. As the authors admit early on in the report, they made no assumptions about the "compensating controls or procedural mitigation measures that vendors, the Secretary of State, or individual counties may have adopted." [34] Moreover, the authors acknowledge that the "testers did not evaluate the likelihood of any attack being feasible." [35]

Similarly, the claim that paper receipts are needed for voters to believe that the DRE voting machine has cast the correct ballot reflects a naive view of elections for several reasons. First, as discussed later in this report, paper receipts are not the only form of verification. Second, the DRE voting machines used in elections have been independently tested during the certification process. Independent testing has a crucial role in helping ensure the security of voting machines. EAC has worked with the National Institute of Standards and Technology to develop a National Voluntary Laboratory Accreditation Program to test the functionality, accessibility, and security of voting equipment.[36] Only laboratories that receive this accreditation are authorized to issue a national certification for voting machines, and the vast majority of states require this certification. If independent testers do not find a vulnerability that is later discovered by third-party researchers, then the state should review why the independent testers did not find the vulnerability and work to strengthen the certification process.

Because some people do not understand that voting machines must undergo independent testing, they fear that a voting machine may steal their vote. Independent testers perform quality assurance tests to verify that the machine does not erroneously record voting results. Thus, for example, a DRE voting machine that is preprogrammed to cheat would not be approved by independent testers because it would not give consistent or accurate results.[37] In order to steal votes, the DRE voting machines would have to be compromised after the certification process. The risk of DRE voting machines' cheating can be further mitigated by conducting election-day auditing of a randomly selected group of voting machines during an election. Such auditing provides a probabilistic guarantee that no voting system can cheat.

Election officials use various physical security controls to prevent attackers from tampering with voting machines. Such controls include securely storing and transferring voting machines, using tamper-resistant hardware, and employing election watchers at the poll site. Critics claim that reliance on physical security controls is a weakness; however, paper-based voting systems also depend on physical security controls to avoid cheating (e.g., election watchers must prevent attackers from destroying or altering ballots).

Using a standard refrain from information technology security, opponents of e-voting also charge that "every system can be hacked."[38] They argue that no DRE voting machines should ever be used because any computer can be compromised. This charge is unsubstantiated but plays to many Americans' fears and inexperience with technology.

Once again, the realities of the election process are often ignored. The debate is not whether some machines can be compromised in a laboratory where the attacker has a laptop, tools, and full access to the voting machine, but whether an attacker can alter votes with limited access to the voting machines. Certainly, given enough collusion, time, and access to voting equipment, many attackers could successfully compromise voting machines. However, one of the reasons citizens trust elections is because there is sufficient separation of duties between multiple independent

actors to prevent most types of abuse. Regardless of the voting technology, though, no election is completely secure. To illustrate, "denial of service" attacks can be made against voting machines and poll locations through vandalism or intimidation. Yet the risk from these threats is mitigated by countermeasures, such as the threat of jail. The real threat to elections is from those attacks in which votes can be altered without detection.[39]

Requests for Disclosure of Source Code by Manufacturers

The disclosure of source code by e-voting manufacturers is another contentious issue for opponents of e-voting. Although virtually every DRE voting machine vendor discloses the source code of its products during the certification process, opponents of e-voting claim that it is unfair that everybody does not get a chance to see the source code. Many DRE vendors are unwilling to release their source code publicly because they fear copyright infringement. They also fear that individual reviewers will make unsubstantiated claims against their voting systems prior to an election simply to undermine the public's confidence in the voting systems.

Audit trails are less useful in proving that the voting machines functioned incorrectly. If there is a discrepancy between the audit record and the electronic record, neither voters nor election officials will know which record to trust.

In any event, requiring all e-voting manufacturers to disclose their source code is not the solution. Most computers, including DRE voting machines, rely on third-party software, such as an underlying operating system, hardware drivers, and other related programs. No source code disclosure by a DRE manufacturer will be complete, because DRE manufacturers cannot provide source code for third-party software. Furthermore, attempts to mandate both paper audit trails and source code disclosure miss the fact that if paper audit trails work, there is no need for the source code to be publicly disclosed.

Although Congress should not mandate the disclosure of proprietary source code, states and counties would be wise to show preference to voting system manufacturers that publicly release the source code of their products for review. "Security through obscurity" has long been derided as an ineffective safeguard against attackers. The security of the voting machine should not depend on the confidentiality of the machine source code. Voting systems with publicly released source code will undergo greater scrutiny and testing by security researchers than those that are only tested in government-approved laboratories. Furthermore, voters will have a higher level of confidence in elections conducted on these machines given their greater degree of transparency.

WHY PAPER AUDIT TRAILS ARE NOT THE ANSWER

Requiring that voter-verified paper audit trails be added to DRE voting machines to detect error or fraud will not provide complete security in an election because the integrity of the election still depends on the chain-of-custody remaining secure. The real problem with the current generation of DRE voting machines is not that they use computers, but that the integrity of the election depends on maintaining a secure chain-of-custody of the voting machines and the ballots.[40] This problem is not unique to DRE voting machines, because the integrity of the election in a paper ballot system is similarly dependent on a secure chain-of-custody. In either voting system, a ballot can be compromised only if malicious actors are able to insert themselves into the voting process by, for instance, stuffing a ballot box or changing the code in a DRE voting machine. In both types of systems, election officials employ physical security countermeasures such as locked ballot boxes, poll watchers, and police to mitigate these risks.

Requiring that voter-verified paper audit trails be generated by DRE voting machines would increase the cost and complexity of elections. Paper ballots must be properly created, collected, transferred, tracked, stored, and counted. In addition, printers are costly to add and maintain. Printers can fail for a variety of reasons including hardware failure, paper jams, lack of paper, or lack of ink. Voting machines that generate

"reel-to-reel" paper receipts reduce anonymity on voting machines, especially for the last voters. Since poll watchers can track who votes on each voting machine, a chronological record of votes could compromise voter privacy.[41] Finally, opponents of e-voting demand paper ballots and paper audit trails so that they can be used in a manual recount. Yet manual tallying introduces numerous possibilities for fraud and error given the unpredictable human element.

A voter-verified audit trail provides voters a guarantee that an audit record of their vote was created. The audit trail also provides limited post-election assurance to election officials that the voting machines functioned correctly. An audit trail helps prevent anybody from undetectably altering the ballots cast in an election. Unfortunately, these audit trails are less useful in proving that the voting machines functioned incorrectly. If there is a discrepancy between the audit record and the electronic record, neither voters nor election officials will know which record to trust. Ultimately, election law will determine whether the electronic record or the paper record is counted as the true ballot in a disputed election.

Unlike local verifiability, universal verifiability allows voters to be completely confident in the validity of the final election results.

If a paper audit record is the ballot, as advocated by many opponents of e-voting, then any error or fraud in the paper trail will result in incorrect election results. To steal an election, attackers would merely need to alter the paper ballots and then claim the DRE voting machines malfunctioned. The United States moved to electronic ballots precisely to avoid the problems of paper ballots such as stuffed ballot boxes, spoiled ballots, and stolen ballots. The addition of paper audit trails to DRE voting machines would simply convert our elections back to a paper ballot system. Voter-verified paper audit trails can assure voters that a machine has properly understood their votes, but such audit trails offer no assurances that ballots were recorded correctly or included in the final vote. Similarly, voter-verified paper ballots assure individual voters that their ballot was recorded correctly by a machine, but such ballots do not provide any assurance to voters that their ballot was counted correctly or even included in the final total.

ALTERNATIVES TO PAPER AUDIT TRAILS

Not all audit trails for DRE voting machines are paper based. One option that has emerged is audio verification of votes. After making their selections, voters hear an audio playback of their intended votes over headphones. An audio recorder, independent of the DRE voting machine, then records the audio confirmation of voters' selections. A recent study that compared the behavior of voters on DRE voting machines with audio audit trails and paper audit trails found that the paper audit trails had serious usability defects. The DRE voting machines were configured intentionally to introduce errors into the voting record. The study found that voters were 10 times more successful at finding errors when they heard their vote read back to them than when they read a paper receipt.[42]

Another option is to use two machines: one to record the ballot and a second, independent machine to verify the ballot and create a digital audit trail of each vote. The ballot can be stored on either digital media or paper. Thus, for example, voters could go to machine A to record their ballots onto a smartcard, and then go to machine B to verify that the smartcard contained the correct votes. The security of a system such as this would depend on the two machines not colluding. To discourage collusion, states could require separate manufacturers for each device or use open-source code. The fact that both machines would use audio technology would mean that everyone, including people with disabilities, could independently verify the audit trail. In contrast, paper audit trails would not allow blind or illiterate voters to verify their ballots independently.

A similar form of verification for DRE voting machines could also be achieved by using a single-input, dual output voting system. In this scenario, two independent DRE voting machines would connect to a single input, such as a keyboard or touch-screen. The two separate machines would independently capture all voter input and create separate audit trails of all votes. Again, the security of this voting system would depend on the machines' inability to collude.

An alternative to "local verifiability," where the correctness of each vote is verified by the individual casting the vote is "universal verifiability," which allows anybody to check that the final tally of votes is correctly computed.[43] [44] Unlike local verifiability, universal verifiability allows voters to be completely confident in the validity of the final election results. The simplest example of universal verifiability is a vote taken by a show of hands. Anyone voting or observing the election can confirm that all votes were counted correctly. Obviously, showing hands would not work well in large elections, and it would force voters to give up their privacy. As discussed below, however, several cryptographic procedures have been proposed that provide universally verifiable elections, while also preserving the institution of secret ballots.

MOVING BEYOND PAPER TRAILS: THE NEXT GENERATION OF DRE VOTING MACHINES

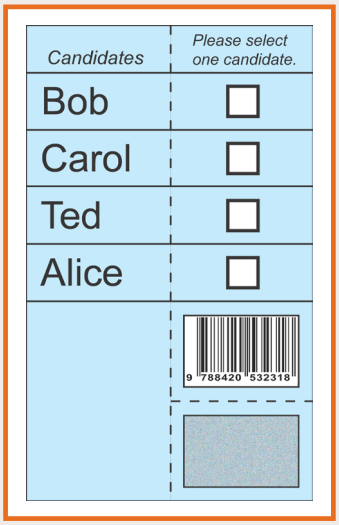
DRE voting machines that provide universal verifiability offer more security than any voting machine currently used in U.S. elections. Researchers have developed a number of proposals to provide universal verifiability using cryptographic techniques (see Box 2) to secure information. These cryptographic systems provide voters with more security and verifiability than is found in traditional voting systems. To illustrate how cryptography can be used to improve the voting process, two examples of voting systems that offers universal verifiability through innovative cryptographic techniques—VoteHere and Scratch & Vote—are described below.

VoteHere

VoteHere, developed by Dategrity Corp., is an example of a voting system that offers universal verifiability through innovative cryptographic techniques. This system gives election administrators a complete end-to-end audit capability and voters the opportunity to verify that their vote is included in the final tally. A simplified version of the voting process includes the following steps:

1. Voters cast an electronic ballot in the voting booth using a DRE voting machine.
2. Voters receive a receipt, which provides them assurance that their ballot was encrypted correctly. The receipt also allows voters to track their ballot on the Internet. This receipt does not provide any information that would allow a voter to prove to anybody else how he or she voted.
3. At the end of the election, election officials post every encrypted ballot on the Internet. Voters can verify that their ballot has been recorded, but they cannot view the details of their ballot. Since the ballots are encrypted, each vote remains private.
4. Voters use the receipt they received after voting to verify that their encrypted ballot was transmitted successfully from the poll site to the central computer and has not been altered.
5. Election officials anonymize the ballots. They use a cryptographic technique called mixnets (described in Box 2) to guarantee that no votes are added or changed.
6. Election officials decrypt and count the anonymous ballots.

Dategrity Corp has published the source code used in the VoteHere system. In addition, it has published a number of white papers that explain, in depth, the details of the cryptography.[47] Although not everyone may understand or want to know the specific mathematics behind this voting system, the availability of the details of this voting protocol provides the opportunity for anybody to verify the security of this system.



Scratch &Vote

Scratch & Vote is another voting protocol that illustrates how researchers are developing innovative solutions for integrating advanced cryptography into easy-to-use voting systems. It uses everyday technology such as barcodes and

a scratch surface (such as that found on a lottery ticket) to provide universal verifiability.[48]

Voters mark their vote on a paper ballot but then cast their vote using a digital image of the Scratch & Vote ballot. This system illustrates how integrating cryptographic voting solutions can create an unprecedented level of security and verifiability for voters.

The Scratch & Vote ballot has two halves, as shown in the accompanying figure. On the left half, the ballot lists the candidates in a random order. The right half of the ballot is a column of corresponding checkboxes. It also includes a bar code, a scratch-off area and a tracking number. The bar code indicates which candidate corresponds with each checkbox; however, this information is encrypted using a secret key. The secret key is located under the scratch-off area.

The voting process in the Scratch & Vote protocol works as follows:

1. The voter marks the checkbox opposite the name of the candidate of his or her choice.
2. The voter discards the half of the ballot that contains the list of candidate names. Since the names on the ballot are in a different random order on each ballot, without the list of names, nobody can tell from the checkmark position whom a voter selected.

BOX 2: CRYPTOGRAPHIC TECHNIQUES TO IMPLEMENT VERIFIABLE, SECRET BALLOT ELECTIONS

Some of the most common cryptographic techniques used to implement secure, verifiable voting systems are described below. Although a discussion of the algorithms behind these techniques is outside the scope of this paper, an overview of these common techniques illustrates how cryptographic solutions can improve voting. All of the techniques described can be implemented using public, open cryptographic algorithms that have been peer-reviewed and subjected to scrutiny by the information security community.

CUT AND CHOOSE. Cut and choose is a basic building block of several cryptographic protocols. How can a piece of cake be divided fairly between two individuals? One simple solution to this problem is to allow one person to cut the cake and the other person to select a piece. This approach works because the person who cuts the cake cannot cheat since the other person chooses which piece each person receives. A similar cut and choose technique can be used to ensure that a voting machine cannot cheat without being detected. For example, imagine a voting protocol where the voter is asked to submit an encrypted ballot. If the ballot is encrypted, how can the voter trust that the encrypted ballot is correct? One solution is as follows. The voter makes his or her selections and then instructs the computer to print two different encrypted ballots. The voter chooses one ballot to test and one ballot to put in the ballot box. Next the computer proves that the test ballot correctly decrypts and matches the voter's original selection. After confirming that the chosen ballot decrypted correctly, the voter submits the encrypted ballot. Since the computer does not know which ballot the voter will select to test, it has a 50 percent chance of being caught if it ever tries to cheat.[45]

HOMOMORPHIC ENCRYPTION. Encryption is the process by which information is encoded to provide confidentiality. Modern encryption schemes have two parts: a public encryption function and a private key. The encrypted information is unintelligible to anyone without the key. Voting protocols use encryption to ensure that ballots remain private. Once ballots are encrypted, they can be made public since they are indecipherable without the key. If election officials make encrypted ballots public, then voters can verify that their encrypted ballot arrived unaltered from the poll site. How can election officials tally the votes if the ballots are encrypted? One possibility is first to decrypt all of the ballots, and then tally the decrypted ballots. The problem with this method is that decrypting ballots compromises voter privacy. A better solution is to use a special type of encryption, called additive homomorphic encryption, to encrypt the ballots. Homomorphic encryption is a special type of cryptography in which the sum of two encrypted values is equal to the encrypted sum of the values. Additive homomorphic encryption has a unique property described by the following equation:

Encrypt (A) + Encrypt (B) = Encrypt (A + B)

(continued)

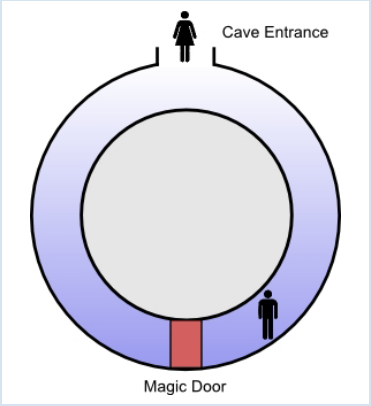
3. The voter takes the remaining half of the ballot to a poll worker. The poll worker ensures that the scratch-off area has not been scratched off.
4. The poll worker detaches and throws away the scratch-off area.
5. The voter scans the ballot into a digital repository. The voter can take the paper ballot home, as it does not show who the voter selected and it does not contain the secret key necessary for decrypting the barcode on the voter's ballot.
6. Election officials post all of the scanned ballots on the Internet, which allows the voter to use the tracking number to verify that his or her ballot is posted online and has not been altered.

To ensure that no ballots are "rigged," each voter can request two ballots during the voting process. The voter audits one ballot and votes with the other one. The audit process works as follows. First, the voter scratches off the scratch-off area, which reveals a key. Using this key, the voter can then decrypt the barcode information and confirm that it is correct (i.e., that the information in the barcode accurately reflects the random order of the candidates on this ballot). Finally, the voter discards the test ballot. Election officials do not accept any ballot where the scratch-off area has been removed.

To tally the votes, a computer reads each barcode to reveal the encrypted value that corresponds to the

BOX 2 *(continued)*

The sum of two encrypted values is equal to the encrypted sum of the two values. This property allows a voting system to add all of the encrypted ballots into a single encrypted tally without first decrypting the ballots. Election officials can then just decrypt this one encrypted tally. Since nobody decrypts the individual ballots, each ballot stays private but the tally is public. How do the voters know the tally was decrypted correctly? The election officials post a zero knowledge proof (explained below), which any voter can verify.



ZERO KNOWLEDGE PROOFS. A zero knowledge proof is a method by which one individual can convince another individual that a statement is true, without revealing anything other than the veracity of the statement. The classic example of a zero knowledge proof involves Pablo the Prover, Violet the Verifier, and a cave with a magic door. As shown in the figure below, the cave is shaped like a circle, with the entrance on one side and the magic door on the other. Only a person who knows the magic word can open the magic door and complete the circle. Pablo wants to prove to Violet that he knows the magic word, but he does not want her to hear the word. Instead, they agree on the following test. Violet stands with her back to the entrance to the cave and Pablo enters either the right or left passage of the cave. Violet then faces the cave and tells Pablo which side of the cave she wants him to exit. If he does not know the magic word, Pablo only has a 50 percent chance of coming out the correct passage. If he knows the magic word, it is easy for him to accomplish. Pablo and Violet repeat this test until Violet is convinced that Pablo must know the magic word. In voting systems, this protocol is useful for confirming that a computer has completed an operation without forcing the computer to reveal information that could compromise voter privacy.

MIXNETS. Universal verifiability means that anybody can verify that the final tally is correctly computed from all valid ballots.[46] To provide universal verifiability, voting systems must allow anyone to look at the final ballots. For example, all of the ballots can be posted on the Internet. Unencrypted ballots cannot be posted online if they identify the voter because this would eliminate voter privacy. One solution is to anonymize the ballots before posting them on the Internet to ensure voter privacy. To anonymize a set of ballots, a computer takes the ballots and outputs a random permutation of them. However, voters need assurance that their ballots have not been changed in the process. Mixnets use zero-knowledge proofs (explained above) to prove that the computer has created a permutation of the original votes, without revealing the selections made by each voter. Mixnets allow voting systems to anonymize data without relying on a trusted third party.

checkmark position on the voter's ballot. Each of these encrypted values was created using homomorphic encryption (described in Box 2 above). This property allows the computer to aggregate all of the encrypted values to arrive at one encrypted tally for each race. Since all of the ballots are available online, anyone can perform these same steps to verify that the election officials have correctly tallied the ballots. Finally, a quorum of election officials decrypts the single encrypted counter, and then posts a proof of correctness that any voter can verify. [49]

Although cryptographic voting systems offer many improvements over current optical scan and DRE voting systems, no voting machine can ensure perfect elections. Even the best voting machine cannot prevent elections from being susceptible to poor authentication of voters, corrupt voter registration databases, and voter intimidation. Nor can these voting machines protect against voter fraud or coercion that occurs through absentee voting by mail. For the voters that use these machines, cryptographic voting systems can offer a significantly improved and more secure voting experience than paper-based systems.

RECOMMENDATIONS

As the 2008 election approaches, members of Congress and state legislatures have introduced a number of bills to address the security of elections and voting machines. Proposed federal legislation, such as H.R. 811 (Rep. Holt, D-NJ) and H.R. 1381 (Rep. Tubbs Jones, D-OH) in the House and S. 1487 (Sen. Feinstein, D-CA) and S. 804 (Sen. Clinton, D-NY) in the Senate, would require voter-verified paper audit trails on all DRE voting machines. We support verifiable audit trails but we disagree that paper is the best solution or should be mandated to the exclusion of other technology. Other proposed federal legislation, including S. 730 (Sen. Dodd, D-CT), requires a verified audit trail, but permits this to be in the form of a paper, audio, pictorial, or electronic record. Similarly, H.R. 2360 (Rep. Ehlers, R-MI) requires that a voting machine allow the voter to verify his or her ballot before it is cast but it does not mandate a specific technology.

Although paper audit trails do provide local verifiability of votes, they are not the only solution. More importantly, they are not necessarily the best solution. A key governing principle of the new economy is that policies should be technology neutral.[50] That means that federal legislation should not restrict states to a single voting technology. It is more desirable to have legislation that requires verification rather than a specific means of verification.

To restore voter confidence and promote secure election technology in the United States by ensuring that states can continue to improve their voting systems, we recommend the following:

- **Congress and the states should allow the use of fully electronic ballots, not restrict electronic voting systems to those that create paper ballots.** Although voting systems still can be improved, Congress should not bend to the intense lobbying of those who would ban any voting machine simply because it is fully electronic. As we have shown, paper ballots introduce many weaknesses of their own and are less secure than more advanced cryptographic voting systems.
- **Congress and the states should require that future voting machines have verifiable audit trails, not require machines with verifiable paper audit trails.** Legislation should not dictate what technology is used in voting machines, but instead define the desired characteristics of voting machines. Congress should allow the U.S. Election Assistance Commission and the National Institute of Standards and Technology to define voting machine technical standards, and not mandate or prohibit any specific technology, including paper trails, wireless communication, and Internet access.[51]
- **Congress should provide funding for the U.S. Election Assistance Commission to issue grants for developing secure cryptographic voting protocols and for pilot testing of new voting technology.** Cryptographic voting solutions offer the promise of more secure and reliable elections. Before appropriating another billion dollars to buy printers for DRE voting machines, Congress should fund pilot programs to test and evaluate new voting technology.

CONCLUSION

Free and open elections are the hallmark of a modern democracy. If the United States wants to continue to be the world's leader in fair, secure, and democratic elections, it must commit to developing improved new voting systems, not go back to the voting technology of the 19th century. We believe that by adopting the recommendations outlined in this report, Congress and the states can restore voter confidence and improve security in our elections.

ENDNOTES

1. The author thanks the following individuals for providing input to this report: ITIF President Robert D. Atkinson and ITIF staff John Anderson, Dan Correa, Julie Hedlund and Torey Liepa.
2. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," exhibition curated by William L. Bird Jr., Washington, DC, 2004 <americanhistory.si.edu/vote/intro.html>.
3. *The American Heritage Dictionary of the English Language*, 4th ed., s.v. "secret ballot" <education.yahoo.com/reference/dictionary/entry/secret+ballot>.
4. Michael Ian Shamos, "Electronic Voting—Evaluating the Threat,'" *Proceedings of the 3rd ACM Conference on Computers, Freedom & Privacy*, San Francisco, CA, March 1993 <euro.ecom.cmu.edu/people/faculty/mshamos/CFP93.htm>.
5. Automatic Voting Machine Company, "Behind the Freedom Curtain" (industrial film), 1957, available at the Internet Internet Archive <www.archive.org/details/Behindth1957>.
6. *Elective Franchise*, U.S. Code, vol. 42, secs, 1973aa-1a.
7. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," 2004.
8. Automatic Voting Machine Company, "Behind the Freedom Curtain," 1957.
9. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," 2004.
10. "For purposes of this Act, paper is 'durable' if it is capable of withstanding multiple counts and recounts by hand without compromising the fundamental integrity of the ballots, and capable of retaining the information marked, printed, or recorded on them for the full duration of a retention and preservation period of 22 months." See *Voter Confidence and Increased Accessibility Act of 2007*, 110th Cong., 1st sess., H.R. 811.
11. For a complete discussion of the election, see Robert A. Caro, *The Years of Lyndon Johnson: Means of* Ascent (New York: Vintage Books, 1990), 209-384; and Merle Miller, *Lyndon: An Oral Biography* (New York: G.P. Putnam's Sons, 1980), 116-137.
12. Robert A. Caro, *The Years of Lyndon Johnson: Means of* Ascent (New York: Vintage Books, 1990), 320.
13. *Help America Vote Act of 2002*, Pub. L. 107-252, 42 U.S.C. 15301 *et seq*.
14. *Help America Vote Act of 2002*.
15. *Help America Vote Act of 2002*.
16. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2003 Annual Report* (Washington, DC: 2003) <www.eac.gov/annualreport_2003.htm>.
17. Wendy R. Weiser, "Are HAVA's Provisional Ballots Working?" Brennan Center for Justice at NYU School of Law, New York, NY, 2006, <www.brennancenter.org/dynamic/subpages/ download_file_39043.pdf>.
18. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2006 Annual Report* (Washington, DC: 2007) <www.eac.gov/docs/EAC%20AR2006.pdf>.
19. Election Data Services,"Voting Equipment Summary by Type as of 11/07/2000," Washington, DC, 2 Feb. 2004 <www.edssurvey.com/images/File/VotingEquipStudies%20/ve2000_report.pdf>.
20. Election Data Services, "Almost 55 Million, or One-Third of the Nation's Voters, Will Face New Voting Equipment in 2006 Election," press release, 2 Oct. 2006 <www.edssurvey.com/images/File/VotingEquipStudies%20/ ve2006_news.pdf>.
21. Election Data Services, "Almost 55 Million…," 2 Oct. 2006.
22. Farhad Manjoo, "The Case for Electronic Voting" *Wired,* 14 Nov. 2000 <www.wired.com/politics/law/news/2000/11/40141>.

23. Bob Shrum, interview by Stephen Colbert, *The Colbert Report*, Comedy Central, 26 July 2007.

24. *Schade v. Maryland State Board of Elections* (2004), Circuit Court for Anne Arundel County <news.findlaw.com/hdocs/docs/elections/schadevmd90104opn.pdf>.

25. *Schade v. Maryland State Board of Elections (*2004).

26. Melanie Warner "Machine Politics In the Digital Age," *New York Times,* 9 Nov. 2003 <http://query.nytimes.com / gst/abstract.html?res=F70E12FD385D0C7A8CDDA80994DB404482&fta=y&archive:article_related>.

27. Tom Spring, "Can You Hack The Vote?" *PC World*, 5 Aug. 2004 <www.pcworld.com/article/id,117261-page,1/article.html>.

28. Stuart Miller, "Don't Trust Computers with e-Votes, Warns Expert," *Guardian Unlimited*, 17 Oct. 2002 <www.guardian.co.uk/internetnews/story/0,7369,813223,00.html>.

29. Alan T. Sherman et al., "An Examination of Vote Verification Technologies: Findings and Experiences from the Maryland Study," *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006,* Vancouver, BC, Canada, 2006 < http://www.usenix.org/events/evt06/tech/>.

30. Tom Zeller Jr., "Why We Fear the Digital Ballot," *New York Times*, 26 Sept. 2004 <www.nytimes.com/ 2004/09/26/weekinreview/26zell.html>.

31. According to Avi Rubin, "[e-voting] makes the job of a person who wants to cheat a lot easier. If the machines had a paper trail, anyone could inspect the outcome, because the paper would give you the right answer." Source: Stefan Lovgren, "Are Electronic Voting Machines Reliable," *National Geographic News*, 1 Nov. 2004 <news.nationalgeographic.com/news/2004/11/1101_041101_election_voting.html>.

32. Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century* (Renton, WA: Talion Publishing, 2004) <www.blackboxvoting.org/bbv_chapter-5.pdf>.

33. California Secretary of State, "Elections and Voter Information: UC Red Team Reports," Sacramento, CA, 2007 <www.sos.ca.gov/elections/elections_vsr.htm>.

34. Matt Bishop, "Overview of Red Team Reports," Sacramento, CA, 2007 <www.sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf>.

35. Matt Bishop, "Overview of Red Team Reports," 2007.

36. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2006 Annual Report,* 2007 .

37. Another possibility is for the DRE voting machine to be configured to cheat only after receiving some activation code, such as a sequence of keys. This type of attack should be mediated against by reviewing the source code during the certification process and election-day auditing.

38. Christina Almeida, "Expert Issues e-Voting System Challenge to Hackers," *USA Today*, 30 July 2004 <www.usatoday.com/tech/ news/computersecurity/2004-07-30-evote-hack-challenge_x.htm>.

39. Michael Ian Shamos, "Electronic Voting—Evaluating the Threat," 1993.

40. Ben Adida, *Advances in Cryptographic Voting Systems,* CalTech/MIT Voting Technology Project, VTP Working Paper #51, September 2006 <vote.caltech.edu/media/documents/wps/vtp_wp51.pdf>.

41. Contemporaneous reel-to-reel paper receipts reduce anonymity for all voters. See Michael Ian Shamos, "Testimony Before the Maryland General Assembly House Ways & Means Committee," 2004 <euro.ecom.cmu.edu/people/ faculty/mshamos/WaysMeansTestimony.htm>.

42. Sharon B. Cohen, "Auditing Technology for Electronic Voting Machines,"CalTech/MIT Voting Technology Project, VTP Working Paper #46, May 2005 <www.vote.caltech.edu/media/documents/wps/vtp_wp46.pdf>, 5.

43. Ben Adida, *Advances in Cryptographic Voting Systems,* September 2006.

44. *CyberVot*e, "Frequently Asked Questions: 5. What is Universal Verifiability?" n.d. <www.eucybervote.org /faq_security.html#q33>.

45. The voter cannot vote with the decrypted ballot because he or she would know the keys used to decrypt it. In most voting protocols, the computer encrypts the final ballot using keys unknown to the voter so that the voter is unable to prove to a third party how he or she voted. This requirement prevents voter intimidation and vote selling.

46. *CyberVot*e, "Frequently Asked Questions…"

47. See for example, the following: Andrew Berg, "VHTi Verification as a Scratch Ticket," VoteHere, Inc., Bellevue, WA, 2004 <www.votehere.net/vhti/documentation/VHTi_Cryptography_Explanation-detailed-2.0.3638.pdf>, C. Andrew Neff, "Verifiable Mixing (Shuffling) of ElGamal Pairs," VoteHere, Inc., Bellevue, WA, 2004 <www.votehere.net/vhti/documentation/egshuf-2.0.3638.pdf>; and C. Andrew Neff, "Practical High Certainty Intent Verification for Encrypted Votes," VoteHere Inc., Bellevue, WA, 2004 <www.votehere.net/vhti/ documentation/vsv-2.0.3638.pdf>.

48. Ben Adida and Ronald L. Rivest, "Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting," *Proceedings of the 13 ACM Conference on Computer and Communications Security (CCS'06)*, Alexandria, VA, 2006 <ben.adida.net/ research/AdidaRivest-scratch-and-vote.pdf>.

49. Ben Adida and Ronald L. Rivest, "Scratch & Vote…", 2006.

50. The New Economy Task Force, "Rules of the Road: Governing Principles for the New Economy," Progressive Policy Institute, Washington, DC, 1999 <www.ppionline.org/ppi_ci.cfm?contentid= 1268&knlgAreaID=128&subsecid=174>.

51. The *Voter Confidence and Increased Accessibility Act of 2007*, 110th Cong., 1st sess., H.R. 811, for example, would prohibit voting machines that allow wireless communications or that have been connected to the Internet.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with ITIF specializing in issues relating to IT and the digital economy. He has experience in the private, non-profit and government sectors. Outside of ITIF, Mr. Castro is a Visiting Scientist at the Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania where he has developed virtual training simulations to provide clients with hands-on training of the latest information security tools. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.innovationpolicy.org.
ITIF | 1250 I St. N.W. | Suite 200 | Washington, DC 20005