A Proposal to Restore Integrity and Confidence in Our Electoral System and to Empower Voters

Barry Cohen and Ira Cohen

Introduction

A democratic society must secure its elections against tampering or significant error by election authorities or by private parties. Equally important, the public must be confident of the integrity of elections. Yet all electronic voting systems currently in use are at substantial risk of tampering. A significant section of the public now feel that their votes may not be accurately recorded and/or counted. By these measures, democracy has been severely eroded in our country in recent years.

VoiceVote (**Vo**ting **I**ntegrity, **C**onfidence and **E**mpowerment) is an easy-to-understand, transparent voting system that addresses both the reality of electoral integrity and public confidence in it. VoiceVote presents all computer programs it uses for public review and verifies that the programs it uses are exactly those that have been approved, providing the highest degree of certainty as to their correctness. All ballots are completely anonymous with nothing to link the ballot to the voter. VoiceVote produces an unalterable electronic record of votes cast and two complete paper trails: one retained by the voting authority in a sealed ballot box and the other in the possession of the voter. The voting authority tags and cryptographically certifies each ballot as it is cast and provides every voter a receipt detailing their choices on the ballot. The voting authority publishes all ballots on the Internet immediately after the election.

This system enables each voter to anonymously check that his or her vote has been correctly recorded and prove any instance of a vote being lost or altered. In this way, VoiceVote empowers voters to directly monitor the integrity of every election. The cryptographic certification also prevents any baseless accusation of fraud and provides a powerful tool for the suppression of vote buying.

The democratic maturity of our nation has grown during its more than two centuries. People increasingly believe that they should have the right to see into government processes. These expectations have given rise to sunshine laws and freedom of information acts. The principle of "one person - one vote" has gradually become more widely accepted and implemented. Failure to correctly count every vote is a grievous violation of this principle.

The election systems we design should meet the challenge of democratic expectations. Giving the voters themselves an independent capacity to guarantee that their votes are counted correctly should be seen as a continuation of the historical process of expanding and reinforcing the democratic content of the electoral system. VoiceVote replaces the "Voters Keep Out" sign on the door of the vote counting room with a "Voters Welcome" sign.

Principles of VoiceVote

The development of democracy in America is an unfinished and ongoing process. Democracy is about much more than elections and elections are about much more than voting. However, it is reasonable to chart the growth of our democracy by the expansion (and sometimes contraction) of voting rights and the ability of the election system to express the intent of the electorate.

Voter expectations regarding election integrity are not static. Rather, they are shaped by the same forces, including the explosion of information technologies, that have given rise to demands for greater transparency in all types of government operations. Voters today expect every citizen to enjoy equal access to an election process that is free from error and corruption. By that standard, the gap between voter expectations for American democracy and the reality of our electoral system has taken a turn for the worse in recent years.

The elections of 2000, 2004 and 2006, and especially Bush v. Gore, highlighted this crisis of confidence. The actions of the courts and the Congress have done little, if anything, to alleviate the growing distrust of many Americans with the ability of the electoral system to reflect their will, to represent their interests and to accurately and reliably record and count their votes. As reported in a CalTech/MIT Voting Technology Project working paper Are Americans Confident Their Ballots Are Counted?

The issue of trust and confidence in the electoral process looms large in the United States in the wake of the disputed 2000 presidential election, especially following the many reports and studies of procedural irregularities, mistakes, and problems associated with the counting and recounting of ballots in Florida and other states.

The Project found in that issues of confidence and trust persist today:

> Despite efforts at reform, including passage of the "Help America Vote Act" in 2002, questions persist about the degree of confidence and trust that American citizens and voters have in their electoral process,given that problems again arose in the 2004 presidential election in a number of states, including the pivotal state of Ohio.

In a report titled Challenges Facing the American Electoral System: Research Priorities for the Social Sciences, the National Research Commission on Elections and Voting notes:

> It is the view of this Commission that significant reforms in American electoral institutions are very much needed at this juncture in American political history. There is ample evidence that our electoral system does not match – and sometimes frustrates – the promise of American democracy. There is also abundant anecdotal evidence that many Americans have lost confidence in the fairness and neutrality of our electoral processes: one of the more notable features of the weeks immediately following the November election was the proliferation of theories and claims that the presidential election had been stolen.

VoiceVote is designed to address this acute problem by implementing principles that have historically been the goals of democratic elections:

* **Anonymity**. The voter alone should decide whether and what to disclose about the choices made on the ballot. The voter should have the right to choose whether to disclose nothing, to disclose their vote or even to make false statements about how they voted.

* **Accuracy**. There should be clarity in the presentation and marking of ballots, so that they represent the true intent of the voter, and there should be zero tolerance for errors in the recording and counting of votes.

* **Transparency**. Voters should be able to see and to understand all aspects of the system, and the maximum possible amount of information about all votes cast, consistent with the principle on anonymity, should be made public.

* **Confidence**. Every election should be subject to quick, reliable and automatic verification, and there should be effective recourse in the event that the integrity of the system is shown to have been compromised.

The key to the VoiceVote system is that it brings the public directly into the process of verification. It creates and gives to each voter a cryptographically certified paper record of their vote, tagged with a random identifier, which the voter may compare to the complete set of votes posted on the Internet. This receipt enables each voter to check that their vote is correctly recorded. If a voter's ballot is missing or altered, it gives the voter a way to prove the error or fraud. Any voter may independently count every vote throughout the country. VoiceVote employs technologies that are already in wide use: public key signatures - an established method of verifying the authorship and integrity of documents - and the Internet.

The VoiceVote system consists of specifications for equipment, software and procedures for the conduct of elections which, taken together, improve the security, accuracy and efficiency of elections. Within this framework, VoiceVote permits election authorities, vendors and implementers wide latitude. The VoiceVote system elevates the role of voters to co-guarantors with the election authorities of the integrity of the system as well as decision makers.

Wherever possible, VoiceVote preserves familiar election procedures. For example, voters go to a local polling place to cast their ballots. While VoiceVote retains time-tested aspects of voting procedure, it recognizes that the technology of voting is changing, and uses proven and practical technologies to enhance the electoral system.

Key Features of VoiceVote

The VoiceVote system uses established and proven technologies to do three things reliably and securely: i) permit the voter to privately and accurately register his or her intent on each ballot question, ii) label and cryptographically certify each ballot so that it can be tracked through the final vote count; iii) provide redundant audit trails so that the accuracy of the entire election process can be independently examined by both the voting authority and the voting public.

The following features of VoiceVote support these goals:

* **Use secure, publicly reviewed software**. All programs used by VoiceVote, including the operating system, are available in advance for public inspection, in both human readable and machine readable forms, bringing the collective expertise of the professional computing

community to bear on their correctness. The software is installed on ROM (Read Only Memory) chips that cannot be altered. The appliances are tested on startup at the beginning of the voting session to assure that the approved software is running and can be tested throughout the course of Election Day. The VoiceVote voting machine is not connected to any network to prevent the possibility of "hacking." The equipment contains no disk drive or other persistent, rewritable memory.

* **Improve voting accuracy through friendly design**. The VoiceVote voting machine has a touch screen (ATM-style). This permits any size or style ballot, in any language. Good ballot design can make voting on a touch screen very clear and user-friendly. The machine can be tailored to facilitate voting by the physically- or vision-impaired. The voting software prevents overvotes, in which the voter accidentally marks the ballot for two candidates for the same office. By calling attention to omitted votes, it greatly reduces the frequency of undervotes, in which the voter unintentionally fails to vote on some matter. Undervotes, such as those that appear to have occurred in 2006 in Florida's 13th Congressional District contest, have been a major source of the failure to correctly record voter intentions.

* **Label and cryptographically certify each ballot**. VoiceVote software labels each ballot with a unique random identifier, enabling it to be tracked after it is cast, much as the identifier on a package enables its progress toward its destination to be tracked. Each ballot is digitally signed, guaranteeing that any loss or alteration of ballots can be detected. The ballot label is not connected to the identity of the voter and does not compromise the anonymity of the ballot.

* **Create multiple audit trails**. The VoiceVote voting machine records each ballot in three independent, cryptographically certified trails: an electronic record and two paper trails. Each ballot, in whatever form it is recorded, contains the ballot identifier and the cryptographic certification. The electronic trail is created on a write once (WORM) medium, which cannot be altered. One paper trail is deposited in a sealed ballot box and is retained by the election authority. The other paper trail is given to the voter. The cryptographic certification permits detection and proof of the alteration or loss of any ballot. It also prevents ballot forging. This gives the voters, as well as the election authority, the power to independently audit the election.

The VoiceVote Vote system is **vendor-neutral**. Any manufacturer may produce appliances and programs adhering to this voting protocol, making it less likely that the manufacture of voting machines will be monopolized. This should help keep down the costs of the system and preclude the possibility of partisan ownership of crucial components of the election apparatus.

Empowering Voters to Verify Election Results

In the VoiceVote paradigm the voter is assumed to be an informed public observer, whose confidence in the fairness and accuracy of elections is crucial to the health of our democracy. Further, the voter can actively test and enforce election integrity. VoiceVote runs "sunshine elections." All the information that the public needs to vet an election is proactively provided as a matter of right.

Transparency and anonymity are the critical features of the VoiceVote system. The creation of a paper trail for voters and the publication of all ballots -- without any identification of the voter who cast each ballot -- and other election information on the Internet enables the voting public to confirm the integrity of each vote and of the election process as a whole. The information published on the Internet includes each ballot, with its unique ballot identifier and signature, each voting session identifier and session verifying key, a tally of the votes for each candidate and/or question on the ballot and the cryptographic certification of the program source code. Using this information, the public can verify every election, without the need for a court ordered recount.

All ballot records are cryptographically certified, which means that they are unforgeable and that any tampering can be detected. Unlike some other proposed cryptographically based systems, the voter's anonymity is not dependent on the strength of the cryptography. The identity of the voter remains secret even if the cryptography is broken.

After the polls close and the results are published on the Internet, any voter may go online and perform these basic audits of the election:

* **Check their own vote**. Any voter may look up the ballot that matches the unique identifier on their ballot. (Note: this is an identifier of the ballot, and has no connection to the identity of the voter.) The voter enters this identifier, and the election authority displays the corresponding ballot. The ballot identifier could be barcoded on each printed ballot, permitting it to be easily read.

* **Check against ballot box stuffing**. Anyone may compare the number of ballots cast in each precinct to the number of applications for ballot issued by the voting authority. The two numbers must be equal. This provides a safeguard against ballot box stuffing. This safeguard is generally present in current election procedures, but not in a form readily accessible to the public.

* **Check against ballot tampering**. Anyone may download a complete sets of ballots for any jurisdiction and confirm that each one is authenticated by the digital signature of the corresponding voting session. Even the smallest alteration of a ballot will be detected by the digital signature.

* **Check that all votes are correctly counted**. Anyone may download the complete set of ballots in any electoral jurisdiction and conduct an independent tally of the votes on each ballot question.

* **Anonymously challenge missing or altered ballots** by providing a copy of the receipt to a representative, the election authority or law enforcement or by pointing out instances in the public record of ballot box stuffing or ballot tampering.

* **Participate in a group**, each of whom checks their own ballot anonymously and/or assists others in checking their ballots (e.g. vision impaired to confirm that ballots marked by voice were correctly recorded)

* Before and after each election **check the software used by the election** including operating systems and algorithms for digital signatures and ID generation or consult with experts of choice who have examined the software without having had to sign a non-disclosure agreement.

Large numbers of voters may be expected to check their own ballots in an elementary exercise of democracy. The participation of any significant number of voters in auditing the election, using their cryptographically certified paper trail, makes it extremely unlikely that any systematic alteration or discarding of votes will go undetected. A single lost or altered ballot is all that is required to trigger a full-scale official investigation and recount.

Two Paper Trails Are Better Than One (or None)

The VoiceVote system produces an unalterable electronic record and two separate paper trails. One paper trail is retained by the voting authority in sealed ballot boxes. The other paper trail is retained by the individual voters. These dual paper trails make the election authority and the voters co-guarantors of the integrity of the election process. Each of the ballots in each of these independent paper trails is secured by a digital signature. The two paper trails have identical information, each comprising a complete record of the ballots cast.

The creation of even a single paper trail, in comparison with an electronic voting machine that produces no paper trail, enhances confidence in the security of the election process. However, we consider that a single paper trail that is retained by the election authority is inadequate for four reasons:

First, a paper trail is useless if the paper ballots are not counted, or recounted, in the case of a contested election, and such a count (or recount) occurs only in an official audit. Triggering an audit is generally a difficult, expensive, time-consuming process. Courts tend to be very reluctant to overturn elections, even those with many irregularities. In practice there are few audits. The VoiceVote system builds in automatic, direct voter verification of the integrity of every election. It reliably detects any material error that may occur, and triggers an audit using the election authority's paper trail in the case of a single provably lost or altered vote. Further, the process of the voters themselves checking that their votes are correctly recorded and counted greatly enhances voter confidence in the integrity of the system.

Second, if only a single paper trail is produced and deposited in a ballot box, the voter no longer has any power to independently check his or her own vote. The voter cannot guard against later alteration or wholesale replacement of the vote. This is a fundamental defect of a single paper trail retained by the voting authority. Further, with electronic voting systems it is impossible to guarantee that the paper trail produced corresponds to the electronic votes cast. It is entirely possible for a computer program to display one thing to the voter and to record something different on paper and electronically. Some proposed election systems permit the voter to see (but not touch) a paper ballot that is produced before it is deposited in the ballot box. Tests of this type of system reveal that voters often fail to detect misprinted ballots. VoiceVote gives the voter the ability to print and examine a trial ballot in the voting booth before finally casting a vote.

Third, paper ballot systems that are not cryptographically secured are susceptible to votes being altered, replaced or "lost," as history has repeatedly shown. Voter intent may be difficult to accurately determine from an ambiguously marked paper ballot, and the marks on a paper ballot or may be altered or obscured after the fact. Digital signatures provide a qualitatively higher level of certainty that no information on a ballot has been lost or altered, and are in widespread use in other high security applications.

Fourth , any system that does not permit the voter to retain proof of his or her vote prevents the voter from exercising their role as a guarantor of the integrity of the election. The right to vote is meaningless unless it is backed by the right to guarantee that the vote is properly counted. This shortcoming applies also to some types of cryptographic systems that have been proposed.

The VoiceVote system remedies these problems by building in checks that are integral to the digital form in which the ballot is originally cast. Every ballot has a random identifier that permits it to be tracked. Every ballot has a unique digital signature that guarantees that it cannot be altered without detection. The identifier and signature are integral to each ballot. These, together with the second paper trail in the hands of the voters and the public reporting of all ballots, enable each voter to directly check that their ballot has been accurately recorded. It is no coincidence that, when asked, voters strongly prefer the option of a cryptographically certified receipt that they can retain over a paper trail retained by the voting authority.

The Evolving Standard of Voting Rights

At the time our Constitution was adopted, more than two centuries ago, the majority of jurisdictions in the United States restricted voting to men of property. John Adams, a founding father, argued, in the same year that the Declaration of Independence was adopted, that permitting men without property to vote would lead to "no end" of similar demands on the part of others, including women and "lads." He made no mention of the fact that slaves, many free Blacks, indentured servants and Native Americans were denied the vote. If one set out down this path, Adams warned, the end result would be to "prostrate all ranks to one common level."

Later, the inimitable Benjamin Franklin posed the contrary hypothetical case of a man who owns a jackass worth $50, and who is therefore entitled to vote. Some years after, the jackass dies. Meanwhile, the man has become more experienced and wiser, but he is no longer entitled to vote. "Pray inform me," asks Franklin, "in whom is the right of suffrage? In the man or in the jackass?"

Adams' position is reflected in the originally adopted Constitution, which contains no guarantee of the right to vote. But the sweep of American history vindicates Franklin. Voting rights, along with social and economic rights, have gradually, often against bitter opposition and with some backtracking, been extended so that nearly all may enjoy this most central of our democratic rights.

Alexander Keyssar, in his comprehensive survey of voting in the United States, notes that the same contradictions pointed out by Franklin drove a broadening of voting rights almost

immediately after the Constitution was adopted. Between 1790 and 1850 numerous states legislated a secret ballot and lowered economic and residency barriers to voting. The process of industrialization gave new and largely unanticipated meaning to the expansion of the franchise as the burgeoning class of workers, often immigrants, began to integrate into the political process.

Perhaps the strongest and most persistent theme in the history of American democracy and voting rights has been the struggle for African American equality. The first wave of that epic struggle peaked with the Civil War and the Reconstruction period. Following the Civil War, which abolished slavery, the Reconstruction's XIVth and XVth Amendments to the Constitution (1868 and 1870) first introduced constitutional treatment of voting rights, profoundly altering the Constitution. The XVth Amendment prohibits denial of voting rights based on "race, color, or previous condition of servitude," and it served as the model for the extension of voting rights to other disenfranchised sections of the population. After prolonged struggle, the XIXth Amendment (1919) similarly prohibited denial of voting rights on account of sex, and the XXVIth Amendment (1971) prohibited denial of voting rights on account of age to those 18 or older.

The history of voting rights has not, however, been an uninterrupted march of progress, and legal enactments have not always resulted in the implementation of real rights. Voting rights have grown and shrunk along with the great struggles for social and economic equality. The defeat of Reconstruction (1876) initiated the period of greatest retreat in democratic rights in United States history, effectively disfranchising most African Americans in the South once again. The intent of the XVth Amendment -- to eliminate voting discrimination on the grounds of race or color -- has gradually, and against bitter and continuing resistance, been realized once again only since the passage of the Voting Rights Act in 1965.

Advances in election systems may also involve compromises, tradeoffs and ambiguities. For example, the adoption of our current familiar secret ballot (the "Australian ballot") in Louisville in 1888 was soon followed by its adoption across the United States. It offered a higher level of ballot privacy, but was a significant obstacle to the participation of many illiterate voters, especially recently freed slaves and foreign born citizens, because it required the voter to read the name of the candidate or party he wished to vote for.

As near-universal suffrage has been established more firmly in law in the wake of the passage of the Voting Rights Act, the struggle over voting rights has increasingly shifted to expanding access to voting, to suppressing fraud and intimidation and to the complete and accurate counting of votes. In this context, VoiceVote contributes to the evolving standard of voting rights.

Voting Accuracy and Honesty

A landmark study by the Brennan Center for Justice notes:

Most Americans would agree that the integrity of our elections is fundamental to our democracy. We want citizens to have full confidence that their votes will be accurately recorded. Given the current tenor of debate over voting system security, this is reason enough to conduct regular

systematic threat analyzes of voting systems. Just as importantly, such analyzes, if utilized in developing voting system standards and procedures, should reduce the risk of attacks on voting systems. As a nation, we have not always successfully avoided such attacks – in fact, various types of attacks on voting systems and elections have a “long tradition” in American history. The suspicion or discovery of such attacks has generally provoked momentary outrage, followed by periods of historical amnesia.

VoiceVote is a alternative to other voting systems that offers significant advantages in the following areas:

* accurately capturing voter intent
* guaranteeing that all votes cast are accurately recorded and counted
* adapting to the needs of disabled voters and multiple linguistic communities
* combating vote fraud
* enhancing voter confidence
* resistance to malicious attacks and errors.

Capturing Voter Intent

VoiceVote combines an electronic touch screen to register votes with the creation of duplicate paper trails. Touch screen voting has been shown to have among the highest accuracy rates. It eliminates the ambiguous marking of ballots that plagues paper ballots. It eliminates overvotes, in which the voter casts more than one vote for an office, and greatly reduces undervotes, in which the voter unintentionally fails to vote on some ballot question.

No system other than VoiceVote adequately addresses the issue of undervotes, which was highlighted by the 2006 vote in Florida's 13th Congressional District. In that congressional contest the margin of victory was 368 votes, while the reported undervote in one single county was 18,382, almost certainly altering the outcome of the election. Because the voting machines in that county did not produce a paper trail of any sort, a meaningful recount was impossible. It is remains unclear whether the undervotes were due to poor ballot design or to voting machine error or fraud.

Even a single paper trail retained by the voting authority would not have resolved this question since such a paper trail could suffer the same inaccuracy as the reported vote total. The second paper trail that VoiceVote provides -- alone among current and proposed voting systems -- would have permitted any voter whose vote was not properly recorded to demonstrate the error and seek appropriate redress.

Adapting to the Needs of Voters

The electronic vote input used by VoiceVote offers the greatest accessibility for people with vision or physical disabilities. Larger type sizes, headphones, Braille printing and voice recognition are among the techniques that make voting without assistance more widely available. Paper ballots and optical scan systems are less flexible in accommodating voter needs.

Electronic vote input permits clean ballot design, such as presenting each issue on a separate screen and using widely recognized visual conventions. It is the responsibility of the election authority in each jurisdiction to follow the guidelines for good ballot design. By making ballot designs available in advance for public review, VoiceVote greatly increases the probability that good design principles will be consistently adhered to.

Electronic voting devices can be programmed to allow the user to choose a ballot in a preferred language, which is critical for equal ballot access by different linguistic communities. It separates making the ballot available in multiple languages from issues of recounts and auditing of election results.

Improving Voter Trust

A substantial proportion of voters currently lack confidence that their votes are accurately counted. This lack of public confidence constitutes a serious corrosion of one of the foundations of representative government. The United States has among the lowest levels of voter participation in the world, which is traceable at least in part to the doubts among voters that their votes count. This reached nearly to the level of a constitutional crisis in the presidential election of 2000, which was resolved by the Supreme Court because of the inability or unwillingness to count contested votes. The disposition of a small number of contested votes resulted in the winner of the popular vote losing the election, underlining the imperative of maximum accuracy and certainty in the counting of every vote.

While there is no hard evidence of widespread vote selling, the existence of this corrupt practice is an expression of profound alienation from the electoral system. VoiceVote contributes to restoring voter confidence in elections by permitting each voter to check that his or her own vote is properly recorded and permits anyone to audit the vote count for any office.

Resisting Attacks on the System

In practice, some of the most basic guarantees of computer system security have either failed to be implemented or have broken down even though the threat of such failure has been clear for some time. Tadayoshi Kohno, Adam Stubblefield and Aviel Rubin analyzed one such system:

With significant U.S. federal funds now available to replace outdated punch-card and mechanical voting systems, municipalities and states throughout the U.S. are adopting paperless electronic voting systems from a number of different vendors. We present a security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. We show that voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal software. Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the

only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a poll worker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. We conclude that this voting system is unsuitable for use in a general election.

All current electronic voting systems "have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections," according to a report by a distinguished panel of security and election experts convened by Brennan Center for Justice. The panel makes a set of recommendations to enhance election security. The VoiceVote system meets and goes beyond the security recommendations of the report.

* The least difficult and most dangerous attacks involve software attack programs. Programming errors or errors by election officials in the use of the equipment may have similar consequences. The Brennan report defines a widely applicable and quantifiable measure of the ease of an attack (or likelihood of an error): the fewer parties required to carry out an attack successfully, the easier it is. Software attacks and errors are particularly dangerous because of the potential scale of their consequences.

VoiceVote secures against malicious or malfunctioning software by implementing the principle of software transparency. All VoiceVote software, in both human and machine readable forms, is made available for public inspection in advance of the election, bringing the expertise of the entire computing community to bear on its correctness. Further, VoiceVote builds in tests that the programs running on voting machines are exactly the programs that have been approved. These measures make software attacks extremely difficult. While these measures are compatible with other voting technologies, no system currently in use makes its computer code public.

Another way of testing against software attacks and errors is to check that the output of the system (the recorded ballot) is the same as the input to the system (the voter's choices). VoiceVote also meets and exceeds the recommendations in this respect. It empowers each voter to check that their own vote is correctly recorded. The digital signature on the ballot can be used to prove any alteration. The action of even a small fraction of the voters performing such checks would make it overwhelming likely that any systematic error or fraud would be detected. In addition, any individual or public body can independently tally the vote on any ballot issue. At each stage of the voting process the appropriate election authorities have similar powerful tools at their disposal to detect fraud or error.

* A paper trail, by itself, is of little security value unless it is checked and unless the uncovering of error leads to effective corrective action. VoiceVote builds in a unique procedure -- a second paper trail -- by which an extensive and automatic audit of election results is performed by the voters, in addition to the security procedures followed by election authorities. This provides significant confidence in election integrity beyond what can be provided by spot checks by election authorities.

The Developing Science of Computer Security

Independently, but in parallel with developments in election security, computer security itself is undergoing rapid and perhaps revolutionary change. A report published by Computing Research Association noted:

> [T]he idea of a defendable perimeter for computer security has become meaningless .... The enemy to defend against may well be a trusted employee acting alone — a trusted "insider" — and not an identifiable external force mounting an attack.

Further, the report identifies as one of the grand challenges of trustworthy computing: "Design new computing systems so that the security and privacy aspects of those systems are understandable and controllable by the average user."

Shortly after the 9/11 attacks William A. Wulf testified before the House Science Committee:

> [T]he Maginot Line model has never worked! Every system ever built to protect a Maginot Line-type system has been compromised--including the systems I built in the 1970s. After 40 years of trying to develop a foolproof system, it's time we realized we're not likely to succeed. It's time to change the flawed inside-outside model of security. ...
>
> Other models could distribute the responsibility for defining and enforcing security to every object in the system. Most research on cyber security is based on the assumption that the thing we need to protect is "inside" the system. Therefore, we have tried to develop "firewalls" and the like to keep outside attackers from penetrating our defenses and gaining access or taking control of it. This model of computer security--I call it the Maginot Line model -- has been used since the first mainframe operating systems were built in the 1960s. Unfortunately, it is dangerously flawed. ...

The VoiceVote paradigm provides the basis for doing two things that no voting system currently in use -- whether paper ballot, optically scanned ballot marking system, or touch screen with or without paper trail -- does: i) enabling a distributed defense against error or fraud, enlisting the knowledge and activity of millions of voters and ii) empowering the voters themselves as guarantors of the elections, thereby enhancing their confidence in the system.

Evolving Meaning of the Secret Ballot

VoiceVote preserves and strengthens the secret ballot in a way that qualitatively enhances the role of voters and the public in securing the electoral system and strengthening public confidence in the system's integrity. It does this by creating and giving to each voter an anonymous, cryptographically certified record of the ballot they have cast. It also focuses a powerful light on the entire election process by publishing all ballots on the Internet.

Until now, voters have been denied a receipt recording how their ballot was cast in all in-person voting. This denial has sometimes been considered an essential aspect of the secret ballot. The

rationale has been that a receipt could become a vehicle for vote buying or coercion. Douglas W. Jones summarizes the standard argument this way:

> We must protect voters from outsiders who might try to punish those who vote "the wrong way" or reward those who vote "the right way". To protect voters from punishment, we must assure the voter that his vote is secret. To protect the public from voters willing to sell their votes, we must be assured that even the voters themselves cannot prove how they voted in order to claim a reward.

This definition reflects the discussion of voting principles at the time the secret ballot was adopted more than 100 years ago and reflects the origins of the Australian Ballot in English law with the adoption of the Ballot Act of 1872 and other related legislation. However, it does not accord with either the popular conception of the secret ballot or with the actual current conduct of elections in the United States. In particular, today many people would not accept the notion that they must be denied a record of how they have voted "to protect the public." The public interest and voters' rights are congruent. A survey of voters shows that they much prefer a paper trail that they can keep to verifying a paper trail in the polling place.

The rapid growth of mail voting is the most obvious conflict between the principle "that even the voters themselves cannot prove how they voted" and the actual conduct of elections in the United States. Clearly, the voter may use a marked mail ballot as evidence of how they have voted.

Mail ballots are subject to coercion. Yet an increasing number of states permit any voter to vote by mail. The practice is so general, even for voters who are not traveling on election day, that it is sometimes called "early voting" rather than the traditional "absentee voting." In California, according to the Secretary of State, "any registered voter may vote by absentee ballot. Rather than go to the polls to cast a ballot on election day, you may apply for an absentee ballot, which you will need to complete and return to your elections official. *All valid absentee ballots are counted in every election in California, regardless of the outcome or closeness of any race.*" (Emphasis in original.)

A special provision in Texas election law permits any person aged 65 or over to vote by mail. It is notable that senior voters may be more vulnerable to coercion than others, yet Texas law nevertheless promotes the public interest by extending a special mail ballot provision to facilitate voting by seniors. Approximately one in four seniors nationwide currently votes by absentee ballot. In Oregon, since 1996 all balloting is by mail. It should be noted that Australia, England, Canada and many other developed nations also allow widespread voting by mail as a means of expanding voter participation.

This change has been widely debated among policy experts and in legislatures. Mail ballots are a cause for debate because they undermine some of the safeguards of the in-person voting process. Whenever a voting authority accepts a mail ballot, it foregos the guarantees inherent in the process of in-person voting, including confirming the identity of the voter and assuring that the voter is afforded the anonymity of the voting booth.

The recipient of the blank mail ballot may give it to another person to complete or may fill it out under conditions that subject the voter to pressure. Therefore, early or absentee voting by mail involves some undesirable trade-offs. However, the desire of legislators (and the public) to make voting easier has outweighed their concerns about voter intimidation or the sale of votes. This is another reflection of the continuing evolution, in law and popular understanding, of the standards of voter rights and the secret ballot. None of the states providing for mail ballots has abandoned the secret ballot.

The popular idea of the secret ballot, and we believe the concept appropriate to contemporary conditions in countries with a strong established democratic tradition, involves the "sanctity of the voting booth." No one may observe you while you are voting. After you have cast your ballot, no one can identify that it is yours. That is the essence of the secret ballot. VoiceVote is entirely consistent with this concept. This embodies an expanded concept, compared to 100 years ago, of voter rights. You -- the voter -- alone decide whether to discuss how you voted, and what to say about it, if anything. VoiceVote is entirely consistent with this concept also.

There is no evidence that there is an increase in vote fraud or coercion with wider mail balloting or early voting. Clearly, voters are not champing at the bit for wider opportunities to sell their votes, but they are deeply concerned and skeptical about the ability of the system to count their votes.

Denial of a receipt to voters is **antiquated, counterproductive** and **contrary to principle**. **Antiquated** because the economic and political conditions of the 19th century -- overbearing big city political machines, company towns, widespread election-related violence -- have changed. **Counterproductive** because it precludes the use of one of the most powerful agents of election integrity -- the voter's knowledge of his or her own vote. And **contrary to principle** because it denies voters what ought to be an intrinsic part of a secret ballot system, and does not invest the decision whether and how to discuss one's vote in the voter.

Aside from whether it is desirable to deny the voter a record of her/his vote, it is also worth examining whether, given existing technology, it is feasible. New digital and materials technologies excel at making images, copying them and transmitting them. The means to do all these things have become small, cheap and ubiquitous. A typical cell phone, for example, could take a picture of a voter's ballot and transmit the image even before the voter leaves the voting booth. Nor, in general, is it illegal for the voter to make and share such a record. Existing laws prohibit anyone else from observing the voter marking his/her ballot. This is an essential part of the secret ballot. But miniaturized camera technology has come to prominence so quickly that the habit of having it always accessible has become well established before the law has even considered its impact. The standard election paradigm requires that the voter be denied a record of the ballot. The existence of small cameras and other mobile electronic devices, many with wireless communication capabilities, poses a significant challenge to election administration to enforce this principle in a socially acceptable way. An attempt to keep the voter's camera out of the voting booth might make the line of people waiting to vote resemble airport security, and have an intimidating effect on the voters.

It is time for our election systems to recognize this reality and to utilize the possibilities for making elections more secure and democratic. **Mail voting has become so extensive and miniaturized camera technology has become so prevalent that, in practice, the rationale for denying a receipt to any voter has been completely discredited.** VoiceVote provides each voter a receipt for their own vote in a way that maintains the voter's anonymity and minimizes any possibility of fraud or coercion. Further, it effectively utilizes the voter's knowledge of their own vote and the voting authority's crytographic certification of each ballot to create a higher standard of electoral integrity.

A Brief Comment on the History of Vote Fraud and Coercion

While contention over ballot counting was acute in the presidential elections of 2000 and 2004, the problem of vote fraud has a long history. The complex struggle against ballot fraud in the U.S. dates back to the historic efforts for "a free ballot and a fair count" following Reconstruction in the South, including the *U.S. v. Reese* and *U.S. v. Cruikshank* decisions of the Supreme Court. As Andrew Gumbel writes in *Steal This Vote*:

> Historically, the zero-sum logic of two-party competition has given rise to a number of abuses at the ballot box, as well as an effort to keep those abuses hidden from the general public. In crunch moments, the attitude has been not only: *They're probably cheating, so we'd better cheat, too. It has also often been: We won't say anything about what they've done, because that will only encourage them to rat on us in return.* It has rarely been productive for a candidate or a party to complain that an election has been stolen, leading as it does to invariable accusations of bad faith, paranoia, and the stirring of needless alarm among voters. Races do get contested, and sometimes overturned, but nobody wins popularity points for dragging the process out through the courts. The understanding, in almost all the great ballot-box standoffs of the past two centuries, has been that a fight is a fight, and the measure of a winner lies in the ability to finish ahead, whether by observing the Queensbury Rules or not.

Worse still are examples of the use of claims of "ballot secrecy" to undermine the right to vote. Because a voter must be literate to cast a written ballot unaided, it has sometimes been used to deny those who could not read (especially former slaves and recent immigrants) the franchise.

The VoiceVote Alternative

The standard argument for denying the voter a receipt asserts that the secret ballot *requires* denying the voter evidence of how he or she voted. This confuses two essentially different questions -- the right of the voter to vote in secret, and the right of the voter to disclose (or to not disclose) how they vote. VoiceVote harmonizes these two basic voter rights by incorporating these elementary principles:

1. The voter marks a ballot in secret. There is no link between the voter's ballot and the voter's identity. No one can determine how any person voted by examining the ballots that are cast. But,

of course, after casting a ballot in secret the voter knows how she voted. We may call this the **First Principle of Voting**.

2. The voter has the right to refuse to disclose how she voted, to disclose how she voted, or to lie about how she voted. This is entirely consistent with the principle of ballot secrecy. We may call this the **Second Principle of Voting**. This right is an essential part of political freedom and should be protected by law and custom.

Perhaps the most dramatic instance of the exercise of the right to disclose was by Senator Wayne Morse of Oregon. The United States Senate, in 1953, had 48 Republican senators, 47 Democratic ones and one independent (Morse had declared himself an independent the previous year). When the Senate convened, Morse, "in the presence of a roomful of reporters filled out an absentee ballot in which he voted for Adlai Stevenson, the Democratic presidential candidate." He then caucused with the Democrats, producing a tie for control of the Senate. Because of Morse's high elected office, his action had great impact, but the significance of the right to disclose one's vote is not limited to elected officials. People routinely discuss their votes if they so choose, and this discussion is an essential part of the texture of everyday democratic political life.

VoiceVote extends the voter's right to disclose and discuss how she voted into a right to determine that her vote is correctly recorded and counted. The key to doing this is to provide the voter with an anonymous, digitally certified record of the ballot cast and to publish the entire set of anonymous, cryptographically certified ballots on the Internet. The voter, utilizing her knowledge of how she voted, may then confirm that the ballot she cast was properly counted. Any person or election watchdog group that comes into possession of a ballot receipt may, utilizing the digital signature, test whether there was error or fraud in the recording of the ballot and -- even without knowing the identity of the voter -- initiate a process of correcting the error or fraud.

In this way, VoiceVote uses digital technologies to empower the public as guarantors of election integrity. It uses the voter's own knowledge and current technologies to secure elections against corrosive and unwarranted suspicions and accusations against the electoral system.

Combating Vote Fraud and Coercion

Combating Vote Fraud

Whenever a vote is cast outside of the guaranteed secrecy of a polling booth, a would-be vote buyer may be able to take physical control of the casting of the ballot. VoiceVote eliminates this practice. All votes, including early and absentee ballots, are cast on VoiceVote voting machines, providing the same certainty that it is the approved voter who votes as on Election Day, and with the same anonymity guaranteed by the protection of a voting booth.

The transparency of VoiceVote undermines the basis of vote buying. VoiceVote provides a means for anyone to print out sample ballots in advance of the election. These sample ballots appear identical to a vote receipt issued after a ballot is cast, including containing a dummy

cryptographic signature. Anyone could produce any number of sample ballots before election day at almost no cost and in unlimited numbers. A sample ballot would only lack a valid digital signature, and could not be distinguished from an actual, valid ballot receipt until after the election was completed and the verifying keys of legitimate voting sessions were published. The would-be buyer of votes would be confronted with a large number of offers of sample ballots, driving down the return on investment in bought votes to near zero.

To ensure that the purchased votes were not merely sample ballots, the vote buyer would be compelled to collect vote receipts (or key information from the receipts) and to record the identities of the sellers. He would have to ask the vote seller to forgo payment until after the election results had been published. The sellers would have no means of enforcing the completion of the transaction. The inescapably low level of trust between buyer and seller would make this form of vote buying unlikely.

Even worse for the vote buyer, the unique digital signature on each ballot would provide a way for law enforcement officials to mark forged vote receipts, much like marking the currency used to pay off a ransom. This would provide a powerful new tool to law enforcement officials to pressure street-level operatives to "roll over" on the political boss who financed a vote-buying operation.

A valid receipt presented for the first time for payment after the election would similarly be of no value, since VoiceVote provides a means by which anyone can easily print a duplicate receipt of any ballot that was cast. A cryptographically certified ballot receipt is proof that a ballot has been cast, but gives no indication who cast it.

Sample ballots would present no threat to the integrity of the election process proper because digital signatures are unforgeable. Sample ballots would be easily and reliably detected after the publication of the verifying keys. Widespread knowledge of the worthlessness of sample ballots after the publication of the verifying keys would serve to enhance popular confidence in the integrity of the electoral system.

Combating Vote Coercion

A good voting system precludes the disclosure of a voter's election choices except by the action of the voter, but it cannot prevent social pressure to disclose (or to not disclose).

To illustrate how VoiceVote serves to insulate voters against pressure to disclose their vote, consider the following example of a coercive atmosphere: Say that Veronica lives and votes in a precinct that is overwhelmingly forest-friendly, and that she herself belongs to the Forest Fanatic Society. Nevertheless, for reasons that seem good and sufficient to her, she votes for Joe Logger for chief forest ranger.

Scenario A: Community pressure. Suppose that an election system is used that does not issue voter receipts (that is, any current election system). If the Forest Fanatics ask each of their

members to state publicly that they voted against Joe Logger, Veronica has three choices: she may refuse to make any statement about her vote, she may disclose it, or she may lie about it.

Now suppose that the VoiceVote system is in effect, and that Veronica has been issued a receipt after casting her vote and that all ballots have subsequently been posted on the Internet. If the Forest Fanatics ask all their members to post their ballots on the community bulletin board, Veronica has exactly the same three options: she may refuse to post any ballot, she may post the receipt for her vote, or she may download a ballot from the Internet that was cast against Joe Logger and post it (that is, she may lie about her vote). There is nothing to distinguish a downloaded ballot from one distributed to a voter at the polling place, and nothing to indicate the identity of the voter on any ballot. Therefore, Veronica's posted ballot no more proves how she voted than a verbal statement. Since it would be common knowledge that anyone could download any ballot, the entire practice of exerting social pressure in this way would be discouraged.

Scenario B: Stolen vote. Suppose that the pro-forest sentiment in this jurisdiction is so strong that the precinct election judges and all the poll watchers collaborate to discard Veronica's vote for Joe Logger. In the VoiceVote system, Veronica can prove that her vote has been discarded by producing her digitally signed ballot and trigger an audit of the election, which would be performed using the election authority's printed paper ballots. What's more, she can accomplish this anonymously by sending her digitally signed vote receipt to a vote integrity organization -- say, the Center for Election Responsibility and Trust (CERT). Veronica's vote receipt in the hands of CERT has the same power to challenge the theft of her vote as in has in her hands. In this way, the VoiceVote system greatly enhances the secrecy of the ballot: it allows a voter whose vote has been stolen to not only effectively challenge the theft, but to do so without disclosing her identity.

Scenario C: Suspicion of stolen votes. Suppose that no votes are actually altered or discarded, but Veronica, knowing the strength of pro-forest sentiment, is suspicious that election fraud has occurred. Under the VoiceVote system, her suspicion is dispelled by the fact that she can confirm that her own vote for Joe Logger was properly recorded and by the knowledge that every other voter can likewise check their own vote and can anonymously challenge any instance of vote tampering.

The VoiceVote protocol is designed with the dual objectives of securing elections against tampering and of giving the public confidence in the integrity of the system. These goals are promoted by the combination of well-established cryptography with simplicity, transparency and direct involvement of the public, including in the post-voting phase of the election.

Further Checks on Election Security

VoiceVote provides powerful tools that enable the election authority to conduct secure elections and to capture voter intentions accurately. It also provides tools for poll watchers, appropriate law enforcement agencies and the courts to verify the integrity of the election process. The most important of these tools is the generation of redundant sets of cryptographically certified records.

Using these records, the following cross checks on election correctness may be performed by the various parties to an election:

Election Authority

* **Integrity checks.** Check the digital signature on each ballot cast to ensure its authenticity. Compare the number of votes cast to the number of votes authorized to be cast by the judges of election. Compare this number to the number of applications for ballot. Compare the preliminary results received on election night with the final results tabulated from the voting appliances after they have been returned. In case of a recount, the duplicate, independent, cryptographically certified paper trail permits an exact comparison between paper and electronic ballots.

* **Election Day spot checks.** Permit the election authority to ensure that the digital signatures used on Election Day are the same as those use to sign the ballots published on the Internet. Also produce evidence that the software running on each machine has not been tampered with.

* **Summary reports.** At the end of the Election Day, VoiceVote produces a digitally signed and therefore unforgeable paper trail summarizing the activity at each polling place, including the vote totals for each candidate and question on the ballot. The election authority compares these summaries with the complete reports produced after the official canvas.

Law Enforcement Authorities

* **Election Day spot checks.** Appropriate law enforcement authorities can initiate spot checks and retain copies of the same spot check information available to the election authority and to the election judges. They can also compare the number of votes cast to the number of applications for ballot.

Poll Watchers

* **Election Day spot checks and summary reports.** Poll watchers are entitled to receive hard copies during Election Day of these same cryptographically certified reports.

The Courts

* **Access to all records.** The courts have access to all of the reports listed above. In addition, voters and the public will have received cryptographically certified information from the VoiceVote system which they may present as evidence to the court.

The twin objectives of an election system should be to conduct secure and accurate elections and to enhance voter confidence in those elections. VoiceVote produces multiple independent audit trails of election activity. Each such audit trail is cryptographically certified and is placed in the hands of voters, election authorities, appropriate law enforcement authorities, poll watchers, or the public. This gives each of these parties the means to detect and effectively challenge defects in the conduct of the election.

Preventing Fraudulent Accusations Against the Voting System

Voting is a compact between voters and government. VoiceVote protects both. By providing multiple means of exposing election errors, the VoiceVote system also protects the election authority and the integrity of the electoral system against false accusations. Accusations of election flaws not supported by hard evidence are not credible. A charge that a particular ballot has been lost or altered is credible if - and only if - the charge is backed up by a paper version of that ballot that has been digitally signed by a VoiceVote voting machine.

Election Day Procedure

Starting a voting session

At the start of the voting session each of these operations are performed once:

* **Start up voting machine.** The judges of election set up and turn on the voting appliance. The appliance performs a self test to validate the software that is running.

* **Initialize cryptographic keys.** All records generated by the VoiceVote system are certified with a digital signature. The digital signature is calculated using the Digital Signature Standard approved by the U.S. government, or other secure scheme for generating digital signatures. The Digital Signature Standard is already in widespread use for applications requiring high security.

The VoiceVote software automatically generates a pair of cryptographic keys: a verifying key and a signing key, which will be used to digitally sign ballots. A digital signature uses one key in the pair to sign a digital document, the other to verify the signature. At the same time that this second key verifies the signature, it also verifies that the signed document has not been altered.

The VoiceVote software immediately records the verifying key on its write once storage medium. It uses the signing key throughout the session to sign each ballot that is cast. The signing key is never recorded on paper or on any other persistent storage medium. VoiceVote does not communicate the signing key or reveal it to any voter or to the voting authority. To safeguard its security, the VoiceVote voting appliance is not connected to any network. The signing key is discarded at the end of the voting session, rendering it impossible to forge signatures for this voting session.

* **Create startup record.** The VoiceVote appliance examines the electronic ballot storage device to make sure the session is starting with zero ballots cast. It creates a digitally signed electronic record along with digitally signed paper records ("zero tape") for the election authority and the poll watchers, attesting to the clean start of the election session.

Casting a vote

The following procedure is repeated for each voter:

* **Authorize a vote.** An election judge authorizes the casting of a single vote on a VoiceVote voting appliance. The VoiceVote machine is locked until a vote is authorized. Each appliance publicly displays a constantly updated count of the number of votes cast, confirming that each voter casts one, and only one, vote and that this vote is recorded. This permits an ongoing comparison of the number of votes cast with the number of applications for ballots.

* **Label the ballot.** The VoiceVote voting appliance assigns a unique random identifier to the ballot. This identifier will be recorded on each representation of the ballot (paper or electronic). It does not compromise the anonymity of the voter because it is not based on any information about the voter.

* **Mark the ballot.** The voter proceeds to mark his or her ballot on the ATM style input screen, with the opportunity to go back and change any choice until the ballot is actually cast. Overvotes are not permitted and the voter is warned of any undervotes before exiting any screen and once again before the voter confirms completion (casting) of the ballot.

* **Digitally sign the ballot.** When the voter has finished filling out the ballot, the VoiceVote machine calculates a unique digital signature for the ballot, based on the ballot's unique random identifier and the way the voter has marked the ballot. The digital signature attests that the vote was cast in a particular election session and has not been altered. The digital signature is integral to each representation of the ballot (paper or electronic).

* **Create electronic and paper trails.** The VoiceVote voting appliance generates an electronic record and two paper copies of the completed ballot. Each copy of the ballot contains both the unique identifier and the digital signature. One paper copy is retained by the voting authority, and can be used to conduct an election audit, if necessary. The other paper copy is given to the voter. Special VoiceVote features guard against use for vote buying. The electronic record is recorded on a write once storage medium in a manner that makes it impossible to determine the order in which the votes were cast. Information that is recorded on a write once storage medium cannot be erased or altered. An example is a write-once CD that is "burned."

Ending a Voting Session

At the end of each voting session each of these operations is performed once:

* **Process absentee ballots.** The judges of election process the absentee ballots, commingling the ballots from qualified absentee voters with the votes cast during the current election session.

* **Produce session report.** The VoiceVote software produces a summary report detailing all unique identifiers, the session verifying key, a tally for each candidate and/or question on the ballot and the serial number and digital digest of the program source. The electronic copy of the report is stored on the write once device and paper copies are produced for the election authority and poll watchers. All reports are digitally signed.

* **Discard the signing key** so no new digital signatures can be created for this session.

* **Freeze the write once device** so no additional records may be written.

* **Copy results to the reporting machine.** Transfer the complete record of the voting session to a VoiceVote reporting appliance, where it is combined with reports from all the other voting machines in the polling place and transmitted to the central election authority.

* **Return equipment.** The voting appliances, with the write-once storage medium and all other read and/or write devices still locked inside, are returned to the central election authority. The central election authority will publish the entire set of ballots on the Internet so that they are available to the public at large. The set of verifying keys will be published along with the ballots. The complete set of ballots and verifying keys may be effectively and cheaply published using, for example, BitTorrent technology.

Absentee and Provisional Ballots

Absentee voting has become a much more widespread practice recently. Advance votes cast at public polling places account for a substantial percentage of votes in some states. U.S. citizens abroad, both military and civilian, may also vote by absentee ballot. The mailed paper ballot system of absentee voting has often prevented these votes from being counted in a timely way and has sometimes led to uncertainty and controversy over the accuracy of the count.

The VoiceVote system makes absentee voting easier, more timely and more reliable.

Absentee ballots may only be cast in advance on a VoiceVote voting machine in a public polling place in the voter's home state, or on a VoiceVote voting machine in a U.S. embassy or any location with a concentration of voters abroad. In any case, duly authorized election officials control the polling place.

The voting procedure for absentee ballots differs from in-person election-day voting only in the following respects:

* Each ballot is recorded on a separate write-once medium, which remains in the possession of the voting authority.

* The ballots, both electronic and paper, are marked as "receipt for absentee ballot."

* The voting authority's copy of the paper ballot is placed in sealed Envelope A. Envelope A, along with the write-once copy of the ballot, is placed in sealed Envelope B. Envelope B, along with the voter's application for an absentee ballot, is placed in sealed Envelope C. Envelope C is delivered to the voter's local jurisdiction. It is mailed to the local jurisdiction in the case that the polling place is a U.S. embassy or other remote polling place.

* On election day, the local election officials open Envelope C, examine the application for ballot and determine if the voter is qualified. If the application is approved, the write-once medium is removed from Envelope B and processed through a VoiceVote voting machine. This

voting machine produces a new digital signature for the ballot, drops a paper copy of the newly signed ballot directly into the ballot box and writes the newly signed ballot to its write-once record. The absentee ballot then becomes indistinguishable from non-absentee ballots cast on that machine. The original paper ballot in Envelope A remains sealed, to be used only if needed for an audit of the paper trail. If the local voting authority finds the voter unqualified, the unique random identifier is posted to the Internet with the notation "Voter not qualified." A disqualified ballot is, of course, not tallied.

VoiceVote handles provisional votes in a manner similar to absentee ballots, except that they are processed in accordance with applicable election law.

Conclusion

Over the past two centuries we have slowly and painfully expanded our notions of democracy to include ever broader segments of our people. The franchise has been extended until, today, virtually all citizens 18 years of age and older are entitled to vote. (The major exceptions are people convicted of felonies and voters in the District of Columbia who can vote but are not represented in the Congress.) This principle is enshrined in the guideline, "one person, one vote." The most urgent demands have increasingly shifted to guaranteeing that every vote cast is properly recorded and counted.

Our national inability to satisfactorily resolve questions surrounding several recent closely contested elections have focused attention on some profound and persistent flaws in the mechanism of our elections. The prime requirement of an electoral system in a democracy is to accurately and convincingly report the outcome of any question put before the voters. Because some will inevitably be dissatisfied with the election results, it is imperative that everyone has confidence in the method of arriving at the results. The repetition of disputed results and methods in successive elections is a signal that the machinery of voting does not meet the standards of the day and requires an overhaul to comply with contemporary requirements. It is a reminder that election principles, practices and technologies, like other political questions, are not settled once and for all, but must be periodically revisited in light of changing circumstances.

Today the public has become accustomed to transactions of all sorts being conducted with the aid of computer technology -- quickly, accurately, reliably and transparently. Yet both traditional "paper" voting systems and the electronic systems that have recently been deployed fail to utilize the best available methods and do not meet the required standards of security, accuracy, reliability and transparency. Outdated conceptions of the principles of voting, which real life has left behind and which no longer reflect the reality of the electoral system, have blocked the modernization of guarantees of electoral integrity. It is unconscionable that voting, democracy's most fundamental act, be conducted with lower standards of security and transparency than the most ordinary commercial transactions.

Aviel D. Rubin writes:

The facilitation and securing of the voting process cannot be left to the private sector, where legitimate concerns about profitability inevitably lead to conflicting priorities. Governments, presumably interested in staying in power, cannot be allowed to act on voting technology without proper public oversight and total transparency. Questions cannot be adjudicated by our legal system, which pits the interest of one side against another in adversarial trials that do not seek to find objective truths. We will find the answers only through a commitment to a publicly funded, nonpartisan, multidisciplinary research initiative in which no individuals stand to gain and yet the entire nation stands to benefit.

America deserves a foolproof voting system. It must be dependable and easy to use. If the machines cannot be guaranteed to be secure, then they must allow for meaningful audits and recounts through a voter-verified record. Whoever designs that system must be able to prove that the system cannot be cheated and be able to explain why to the average eighth-grader. No American should have to trust someone else, someone with obscure expertise regarding the integrity of the system; it must be simple enough that every citizen can evaluate it for himself or herself. The system must be accessible to all Americans, regardless of disability, and every aspect or component of its workings must be available for public scrutiny.

VoiceVote is a system for recording and reporting votes that addresses the need for higher standards of electoral accuracy by incorporating the following principles:

i) the voter's own knowledge and action is fundamental and irreplaceable in securing elections and in achieving public confidence in the correctness of election results

ii) every aspect of the conduct of elections -- from the computer programs and ballot formats that are employed to the reporting of the ballots that are cast -- should be subject to complete transparency

iii) a secret, coercion free ballot is essential in the democratic process. That ballot should ensure that the voter's choices are never disclosed except by action of the voter, and that the voter has complete discretion whether and what to disclose about his or her own vote

iv) the electoral process should employ the best proven technologies, including cryptographic signatures and Internet communications. It should use only technologies that are already widely deployed and accepted.

Through the implementation of these principles, VoiceVote makes the knowledge and action of the voters themselves central to the solution of the problem of guaranteeing the integrity of election processes and restoring public confidence in our electoral system.

Appendix A: Summary of VoiceVote Procedure

1 The election authority **publishes all software and election specifications**, including templates for the casting and printing of ballots, on the Internet prior to election day.

2 Prior to an election session, the election authority **initializes each VoiceVote voting machine** with the appropriate software, including the applicable ballot template.

3 At the beginning of the election session, each VoiceVote voting machine **generates a pair of private/public cryptographic keys** (signing and verifying keys). The verifying key is written to the machine's write once record.

4 The election judges **generate a start-up report (zero tape)** of vote totals. The report is recorded on the voting machine WORM and printed for the election judges and for all poll watchers.

5 The precinct election judges sign in a voter and **authorize the casting of a ballot**.

6 The voting machine **assigns a random ID** to the ballot.

7 The voter **enters a vote** on the VoiceVote voting machine.

8 The voting machine **calculates a unique digital signature** for the ballot.

9 The voting machine **records the ballot**, including the ballot identifier and digital signature, on a write once storage medium. It prints two copies of the ballot. One copy is deposited in a sealed ballot box for election officials; the voter gets the other.

10 If there is another voter, **loop back to step (5)**.

11 The election judges **process absentee ballots** for the polling place.

12 The precinct election judges **print out a session report** including all unique identifiers, the verifying key, a tally for each candidate and/or question on the ballot and the certification of the program source from each machine for themselves and for each poll watcher.

13 The VoiceVote voting machine **freezes the write once storage medium and discards the private ("signing") key**.

14 The election judges use the VoiceVote reporting machine to **combine and total all results for the polling place** and print digitally signed, hard copy summary reports for the election authority, judges and poll watchers.

15 The election judges use the VoiceVote reporting machine to electronically transmit all of the election results for the polling place, including the ballots and session information, to the election authority.

16 **Return the VoiceVote voting appliances** with the write-once storage medium and all other read and/or write devices still locked inside, reporting machine, sealed ballot boxes and other election materials back to the election authority.

17 The central election authority performs a series of integrity checks on the election information and then **publishes a preliminary report of all ballots and verifying keys** on the Internet.

18 The write once devices are removed from the voting appliances. The **WORMs are read and compared** to the preliminary election results and integrity checks are repeated.

19 **Provisional ballots are processed**. Any discrepancies revealed by VoiceVote integrity checks are investigated and resolved.

20 **Final election results are published**.

Appendix B: Polling Place Hardware

The VoiceVote polling place hardware consists of two types of equipment: the VoiceVote voting machine (VVM) and the VoiceVote reporting machine (VRM). For security, simplicity and reliability the functionality of this equipment is limited to the computational and communication capabilities they require.

The VoiceVote Voting Machine

Hardware:

* CPU
* RAM
* Bus
* Battery backup
* System clock
* Sound card, microphone and headphones for the visually impaired
* Touch screen for voter input
* Output to printers to produce Voter Paper Ballots, Precinct Paper Ballots and other reports
* Output port to transfer data to VoiceVote Reporting machine
* Input-only port connected to Authorize Next Vote switch. This switch requires a key to operate or fingerprint or other biometric identification system, with supporting peripheral hardware. The precinct election judge may authorize the casting of a ballot by an approved voter, a provisional voter or an early or absentee voter on appropriate days before election day
* Output only port connected to Current Vote Count display which displays the number of votes cast on that machine during the current voting session, the precinct ID of the ballot

template in that machine and the status of the machine (standby, ready to vote, voting in progress, vote recorded).

* Input port to read WORM containing previously marked individual absentee or provisional ballot.

* WORM burner to create electronic record for the Central Election Authority (CEA). The recording medium is physically locked and is accessible only by the Central Election Authority. The electronic record includes session information (including machine ID and public cryptographic key) and a complete session set of signed completed ballots. The CEA WORM burner is not accessible by precinct election judges.

* WORM burner (Absentee/Provisional Ballot Burner) with a recording medium to record ballots that are marked by voters who have not yet been approved (absentee and provisional voters) . Each WORM is removed after a single signed completed ballot has been recorded on it and packaged with the corresponding paper ballots. Accessible to precinct election judges.

* Locked case with tamper evident seal for the system (key would not be sent to precinct)

* Suitcase type case for the entire system which would also convert into portable voting booth with appropriate brackets for all displays, switches, speakers etc.

Firmware:

* OS in ROM

* VV voting program in ROM. ROM is physically locked in place and accessible only to the Central Election Authority (CEA). (Could be on same chip as OS.)

* VV ballot template in ROM. Either on a separate chip or pre-burned into CEA WORM and PEJ WORM used to electronically record ballots

* System boot, including routine to verify the content of system ROMs

Things the VVM doesn't have:

* Hard drive, flash drive or other rewritable, nonvolatile memory
* CD/DVD
* Wireless communication capability
* Other ports

The VoiceVote Reporting Machine

Hardware:

* CPU
* RAM
* Bus
* Battery backup
* System clock
* Touch screen for judges' input
* Output to printers to produce reports

* Input port to accept data from VoiceVote Voting Machine
* Locked case with tamper evident seal for the system (key would not be sent to precinct)
* Suitcase type case for the entire system which would also convert into portable booth with appropriate brackets for all displays, switches, speakers etc.
* Cellular communications to Central Election Authority

Firmware:

* OS in ROM
* VV reporting program in ROM. ROM is physically locked in place and accessible only to the Central Election Authority (CEA). (Could be on same chip as OS.)

Things the VRM doesn't have:

* Hard drive, flash drive or other rewritable, nonvolatile memory
* CD/DVD
* WORM burners
* Other ports

Appendix C: Problems With the U.S. Election System Not Addressed by VoiceVote
Some defects in our electoral system require solutions that are inherently political. These problems include:

* unrepresentative districting;
* barriers to universal suffrage either by law or by procedure (most often in the voter registration system);
* lack of an affirmative, constitutional right to vote;
* vote suppression and voter intimidation;
* partisan control of the election process;
* restriction of voting to a single work day and sometimes to a unreasonably limited part of that day;
* campaign financing excesses and inequities
* candidates' lack of access to affordable communication with voters;
* obstacles to ballot access, especially for independents and "third" parties.

Some problems, like the violation of the one-person, one-vote principle in the Electoral College, stand as barriers to the popular will which cannot be repaired but which ought to be removed by constitutional means.

VoiceVote technology may be applicable to certifying voter registrations. However, we do not support this application, because we are convinced that the potential harm from the resulting de facto creation of a national identity card would far outweigh any minimal reduction in false voter registrations.

Appendix D: Mathematical Analysis of VoiceVote

To Be Done