



Internet Voting Panel

CalTech-MIT Voting Technology Conference

March 31, 2001

*Jim Adler
Founder & CEO
VoteHere, Inc.
jim@votehere.net*

I'd like to thank Ron Rivest and the CalTech-MIT Voting Technology Conference Committee for inviting me to participate on this panel. It is a privilege to serve with such distinguished panelists. Debates like this are vital to the national debate on election reform.

Before I get started, a bit about VoteHere. VoteHere has been involved in voting technology since 1996, long before it recently became fashionable. We were founded as a data security company focusing on cryptography and data security products. The voting problem is incredibly challenging and has been researched in academic circles for the last 15 years. Our research and development efforts have resulted in technology that adds real value to the voter. We've conducted both elections trials in 13 states, domestically and abroad, most recently in California and Arizona during last November's Presidential election.

We are owned in-part by Compaq Computer, Cisco Systems, and Entrust Technologies. Recently, longtime Secretary of State Ralph Munro joined our Board of Directors, giving us access to 20 years of election leadership. Since Election 2000, VoteHere has been actively engaged in the election reform dialogue at both the state and national level. In addition to many discussions with members of Congress, state, and county election officials, we've testified before the state legislatures in Michigan, Georgia, Florida, New York, Washington, and Pennsylvania.

Election System Evolution

Elections are undergoing an evolution, accelerated by Election 2000. Voters are demanding greater convenience when exercising their right to vote. Election 2000 saw more absentee votes cast than in any other election, especially out west. 30% of Californians, 54% of Washingtonians, and 100% of Oregonians cast their ballots by mail. In Maricopa County in the Phoenix area, 450,000 of the one million registered voters cast their ballots early.

Military Internet voting

Those that have traditionally been disenfranchised, like the military and disabled, are demanding that their ballot be treated like any other citizen's ballot. Every election reform bill now being considered by Congress requires ADA compliance. The overseas military ballot, often found on the floor due to late or no delivery, is finding a voice. What does it say of our system, if those that defend our democracy cannot participate in it?

Regional voting differences

These reforms will not be enacted uniformly across the country. We have a well-respected, constitutional tradition of state run elections in this country. Election culture and history vary regionally. What works in California may not work in Louisiana. Absentee balloting has not been widely adopted in the east largely due to past voting *irregularities* - irregularities of the coercive and monetary variety. Those

regions prefer to *see* voters enter the polling place, vote, and leave the polling place without influence or evidence.

Evolution roadmap

As the California Internet Voting Task Force report outlined, and the National Science Foundation report recently affirmed, electronic voting will take several forms - from traditional electronic voting at the poll-site, to kiosk voting where any voter can vote at any location, to remote online voting. Various regions and constituencies will adopt the voting system that fits its needs and culture.

For example, county and statewide kiosk voting is gaining support in many east coast states. The ability for any voter to vote at any poll-site is a tremendous leap in enfranchising voters that have been previously shut out. These voters include commuters that leave for work before the polls open and return home after the polls close. In states where absentee voting is difficult, these voters are effectively shut out. With kiosk voting, these voters can vote their neighborhood precinct ballot nearby their worksite during lunch or breaks.

Security Challenges

However, before we get too carried away with this voting utopia, let's remember that every voting convenience along this roadmap presents challenges for security and privacy, if innovative technology is not part of the equation.

Kiosk voting honeybee fraud

Take kiosk voting where any voter can vote at any kiosk. Let's further simplify things by assuming the kiosk is attended by a poll-worker for authenticating the voter. This is the current configuration used for early voting in many states. What are the risks to election integrity or ballot secrecy?

For attended kiosk voting, when the network connection (it could be a private network or the Internet) is even temporarily unavailable (and it will be), an election is vulnerable to what I call the *honeybee fraud* -- a voter can illegally vote at multiple poll-sites since network access to the central poll-book is lost. As a result of this fraud, multiple ballots are cast from the same voter. Traditional DREs cannot deal with these ballots because either (1) the voter name is separated from the ballot or (2) the voter name remains attached to the voted ballot. In the former case (name separated from ballot), removing the correct ballot is impossible since it is mixed with other provisional ballots. In the latter case (name attached to ballot), removing the ballot without violating ballot privacy is impossible since the voted ballot is directly tied to the voter.

Electronic provisional ballot

What's required is an *electronic provisional ballot* that is evaluated during canvassing to ensure that only one ballot exists for each voter. This ballot must be protected so that no one (not election officials, not poll-workers, not the election vendor) can know how the provisional ballot was cast. Implementing this with paper systems requires procedural controls - typically, at least two election officials are required to open a provisional ballot envelope (to make sure no one peeks).

The technology for electronic provisional ballots now exists but is certainly non-trivial. VoteHere announced its shuffle protocol this week that shuffles votes from voters in a way that guarantees election integrity *and* ballot secrecy. I'd be happy to go into more detail during the Q&A.

Electronic balloting already here

Some have recently said that it will be a long time until we vote electronically - in effect, that the train *will not* leave the station. Well, the train has already left the station. Currently, 9% of the electorate votes electronically.

The rhetoric goes something like this: "completely computerized voting systems can give us accountable ballots or anonymous ballots, but not both." Frankly, this conclusion is obsolete. The voting problem *is* deceptively difficult, but as our Chief Scientist Andy Neff says, "Plain, vanilla, electronic storage of ballots

is fraught with problems, but to jump to the conclusion that technologies are not available that solve these problems is reactionary and unscientific."

Electronics should be an electronic paper ballot, not an electronic lever machine

The assumption is that electronic voting systems are electronic lever machines where each ballot increments a set of counters. We dismissed this approach early on as untenable. An appropriate electronic ballot is an electronic paper ballot where ballot images cannot be changed or deleted.

Cryptographic technology has been developed over the past 15 years that solves the security and privacy issues and provides electronic ballots the favorable properties of paper. Many researchers have gotten us to the point where auditable and private voting is possible. We have spent the last five years perfecting this technology for large-scale electronic voting. In fact, we have published some of our early patent-pending work at www.votehere.net/recount.

And speaking of recount, as we are all now aware, election systems need to support exhaustive recount. Any recount must establish three criteria: (1) "legitimate voters" (2) casting "immutable ballots" (3) to produce "repeatable results."

Technology and trust

However, as those of us in the data security world realize, cryptography is just one piece of the puzzle. Good implementation, strict certification, and transparency are critical to a successful voting system. These are the elements that will determine the success of any new voting technology. To date, this approach has not been taken in the industry.

What do I mean by transparency? Well, ultimately what is most important is the public's *trust* in elections. At VoteHere, we didn't go the "trade secret" route that would require us to hide our technology behind non-disclosure agreements and source-code escrow. Instead, recognizing the need to "sunlight" voting systems, we've patented our technology so it will be published for all to scrutinize and understand. We feel the same treatment is important for the source code that runs in our voting machines to prove that the source code reliably implements the patented technology. "Sunlighting" voting technology is a departure from traditional practice in the election industry, but is vital to securing the public's trust.

Paper Voting Systems

Paper voting is a relatively recent phenomenon. The ancient Greeks voted secretly with stones in a bucket - black for no, white for yes. The best part of this system was that it was binary. The stone was either in the bucket or not. No dimpled, hanging, pregnant chads. No half-bubbled, checked, or circled ovals. Voter intent was clear.

This brings me to the two fundamental requirements for a voting system: trust and reliability. First, do we trust that it will accurately communicate the intent of the voter? And second, can we rely on it to perform when needed?

Most of the arguments I hear in favor of paper voting systems are their reliability. Intuitively, paper is low tech and highly reliable. However, as we saw during this last election, complex large-scale elections test this intuition.

Michelle Townsend, Riverside County's registrar, said in recent California state testimony that as a taxpayer and administrator, it was appalling to throw away pallets of unused ballots every election. As most of you know, ballots must be printed for every precinct in adequate quantities for anticipated voter turnout. Unused ballots are thrown away. This ballot-printing burden has been one of the biggest attractions to electronic voting.

Ballot under glass system

But, the history of fragile electronic data has drawn criticism to DREs. Recently, a hybrid system has been proposed that electronically displays the ballot then prints it for voter review before it drops into the ballot box - the so-called *ballot under glass* system. The paper ballot is the auditable record. The electronic ballot is also maintained for fast tabulation.

The arguments for this system are two-fold and are meant to address the trust and reliability requirements. On trust - since the voter reviews the cast paper ballot, he/she knows that their ballot was cast correctly and does not have to rely on the software in the voting computer. On reliability - paper ballots can't be easily erased or lost.

The trust issue gets complicated when you consider how to count the paper ballots. Since the assumption is that computers can't be trusted, the paper ballots must be hand counted since any scanning/counting system can be as easily corrupted with malicious code (e.g., virus, Trojan horse) as the voting machine. For anything other than the smallest jurisdictions, hand counting is infeasible and inaccurate. As Doug Lewis, Executive Director of the Election Center, has said over and over that hand recounts are no solution: "The mind gets tired, the eyes get tired, the body gets tired."

The reliability argument carries more weight and is a reasonable implementation. However, there are other more efficient ways to make sure a cast ballot cannot be deleted. Proposed solutions include writing the data to permanent/redundant media, burning to CD, writing to Write Once, Read Many media, etc.

So, then, what's most attractive about paper is the *perception* that it is more reliable and trustworthy than electronic systems. I don't disagree that perception is important in elections. It is vital.

Take lever machines as an example. They are still used in 15% of U.S. jurisdictions and the entire state of New York. They have no paper audit trail and rely on their physical security to ensure election integrity. However, these machines have been around almost 100 years and are perceived as rock solid. Perception is reality.

Electronic voting advantages

As for electronic voting, software must be certified at development time and the entire software complement verified at election time. Electronic ballots should meet the indelibility requirement - that they cannot be added, deleted, or changed. Logic and accuracy tests must be run just like other systems. And finally, voter intent must be captured accurately. Actually, the voter intent issue is where electronic systems can really improve things.

All voting systems in the field now, rely on two translations from voter intent to tabulated results. The first translation is from the voter's gray matter to the voting medium. The second is from the voted medium (i.e., the ballot) to the tabulated results. The problems in the Florida resulted mostly from the first translation - the voter's intent was recorded ambiguously. The problems in New Mexico were from the second translation - programming error. With electronic systems, the voter can confirm their choices from the ballot image that gets tabulated - in effect, removing the second translation and an entire source of error.

Business Climate

Finally, I want to talk about the changing business climate of election systems. Typically, election systems are procured every ten or more years at high capital expense to the county. Then, every election, ballots are printed at high operational cost to the county. These ballots must be printed differently for every precinct, sometimes in multiple languages. Excess ballots are thrown away.

Sources of error

What is unfortunate about this situation, and unique among elections, is that there is no mechanism to upgrade systems in a cost-effective manner. What's more, given the high accuracy requirements, there

is no mechanism to field corrections once error sources are discovered. This is the situation we find ourselves in today. The most optimistic estimates put the Florida error rate at 1% or about 60,000 votes -- far in excess of the less than 1000 vote victory margin. From a technology perspective, we don't know which presidential candidate won the Florida election.

Election services and upgrade path

Better technology is only part of the solution. Getting the technology in the hands of voters is the real goal. Election services should be offered to election officials, not election equipment. Contracts should be written with provision for upgradeability. When problems are discovered, there should be provision for identifying, correcting, certifying, and deploying those changes. Abandon the large upfront capital procurement structure and embrace a more sustainable service structure. Some jurisdictions are already doing this with great success. We will then have a system in-place that can drive down error when it is discovered.

With 9% of the electorate already voting electronically, the train has already left the station. Our challenge is to keep it on the tracks.