Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Voting Early and Often Can Be a Good Thing

Gerald Post
University of the Pacific

VOTING EARLY AND OFTEN CAN BE A GOOD THING

Gerald V. Post, University of the Pacific, JPost@Pacific.edu

Abstract

The current political climate has almost ruled out the use of Internet voting. Many politicians, led by vocal computer scientists, are pushing for voter verified paper receipts; which is likely to push us even further away from even electronic voting systems. On the other hand, cryptographers have created homomorphic encryption and non-interactive zero-knowledge proofs with features that can support Internet voting. Adding a few more protocols, including an extended voting period and repeat voting can solve the remaining problems need to make Internet voting at least as secure as existing systems.

Key Words: e-voting, Vote, Internet, Security, Risk

Introduction and Prior Research

The voting problems experienced in the 2000 presidential election occurred around the same time as the initial growth of the Web, so several groups suggested that Internet voting could be used for major elections. Some organizations tested the process. Mohen and Glidden (2001) report on the Arizona Republican primary in 2000; Xenakis and Macintosh (2004) discuss the pilot testing performed in the United Kingdom in 2003. In 2000, the U.S. DoD ran an Internet demonstration project in 11 countries according to Garamone (2004). Accenture, in cooperation with the DoD built a system for the Secure Electronic Registration and Voting Experiment (SERVE) with the purpose of helping overseas military personnel vote in elections. The system was put on hold in 2004.

In a relatively short period of time, the tide was turned against Internet voting by several outspoken computer scientists. For example, Jefferson et al. (2004) were on a panel that recommended the immediate termination of the SERVE project. Several other groups, including the California Internet Voting Task Force (2000) have argued against Internet voting. The National Workshop on Internet Voting funded by the NSF essentially concluded that the Internet lacked the security to support voting. Major computing organizations, particularly the Association of Computing Machinery (2004) have strongly recommended against the use of Internet voting, and have even expressly stated that all voting should include some type of physical (paper) record to be inspected by the voter.

The attacks against online voting quickly spread to direct recording electronic (DRE) systems, or computer-based voting systems installed in traditional voting booths. Feldman et al. (2006) and Felten (2006) reported on their dissection of a dated voting machine, and reached the conclusion that voting can be secure only with a voter-verifiable paper audit trail (VPAT). Mercuri (2001) and Mercuri and Camp (2004) has been pushing this point for several years. It is interesting to note that problems were reported (ZDNet 2006) with printers jamming in the 2006 election, including an AP estimate that 9 percent of printers either failed or had paper problems.

These issues have moved the discussion away from the original goals. One of the original reasons for Internet voting was to make it easier for people to vote—hopefully improving voter turnout. One study by Stromer-Galley (2003) revealed comments from participants in a large discussion group. Several suggested that the Internet would make it easier to vote, increasingly the likelihood that they would participate. Of course, there is no assurance that making it easier or more comfortable to vote would actually result in an increase in the number of voters—given the many reasons that people have for not voting. Williams and King (2004) emphasize the usability issue in their study of the DRE voting-booth data provided by elections in Georgia. The electronic systems provided fewer usability errors, and were substantially preferred by the voters. Earlier, Shocket et al. (1991) showed similar results in an experimental design with various ballot technologies.

The goal of this paper is to re-examine the Internet voting approach by looking at the various threats and goals and proposing a method to improve the overall security. This process is shown to be at least as secure as existing system, and more secure than postal absentee ballots, which Phillips and Spakovsky (2001) observe are becoming more prevalent and present a major attack point.

The Election Process

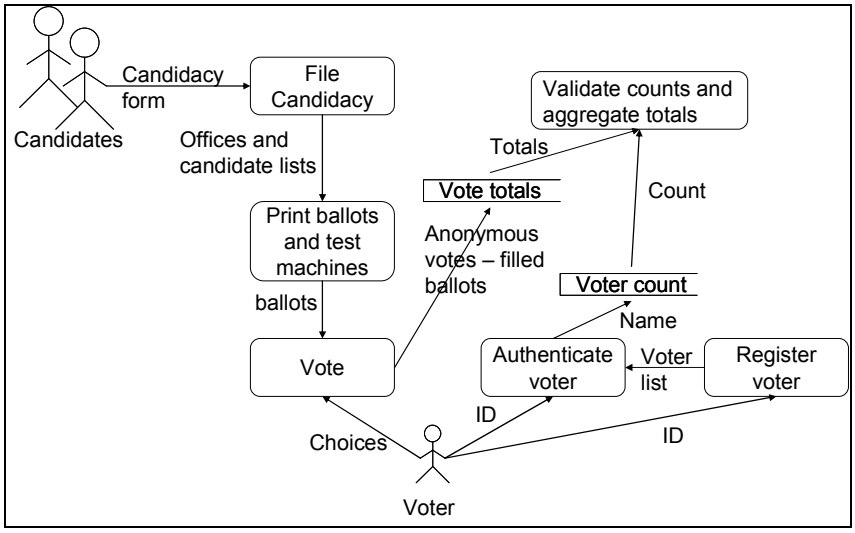

Figure 1. Basic voting process.

The current election process shown in Figure 1 has evolved over decades. Local election officials are responsible for validating the candidates and registering voters. The separation between voter authentication and the vote is important to ensure anonymity of the vote and it is enforced through physical separation. The separate count of the voters provides a check to reduce the probability of ballot stuffing or discarding of ballots. This count can also be compared against the original number of ballots to reduce the risk of vote replacement. In traditional systems, the vote is encoded on paper (usually punch card or optical scan form); providing the means to conduct both electronic and manual counting. In physical systems, voting places are staffed by members of both major parties—with the goal of reducing the probability that election officials are corrupt.

Primary Criteria and Threats

1. Eligibility and Authentication—only authorized voters should be able to vote.
2. Uniqueness—no voter should be able to cast a vote more than one time.
3. Accuracy—election systems should record the votes correctly.
4. Integrity—votes should not be able to be modified, forged, or deleted without detection.
5. Verifiability and Auditability—it should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records.
6. Reliability—election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of communication.
7. Secrecy and Non-Coercibility—no one should be able to determine how any individual voted, and voters should not be able to prove how they voted.
8. Flexibility—election equipment should allow for a variety of ballot question formats (e.g., write-in candidates, survey questions, multiple languages); be compatible with a variety of standard platforms and technologies; and be accessible to people with disabilities.
9. Convenience—voters should be able to cast votes quickly with minimal equipment or skills.
10. Certifiability—election systems should be testable so that election officials have confidence that they meet the necessary criteria.
11. Transparency—voters should be able to possess a general knowledge and understanding of the voting process.
12. Cost-effectiveness—election systems should be affordable and efficient.

Figure 2: Election technology criteria. Source: Internet Policy Institute (2001).

The NSF-sponsored national workshop Internet Policy Institute (2001) identified the 12 criteria shown in Figure 2 as important elements in any election system. Most of these threats have been manifested as attacks at various elections in U.S. history. The current voting-booth solution reduces the risks of all of these threats, but does not eliminate them. Ultimately, most of the security of the existing system depends on the processes and integrity of the local election officials. For example, an official could delay adding a voter to a registration list; preventing (or at least making it more difficult for) a legitimate voter to vote. Similarly, marks indicating a double vote could be added to a legitimate ballot (for the "other" party), causing it to become disqualified. Recording the name of a voter and counting the number of ballots makes it relatively difficult to add unregistered votes at any one location. However, the registration rolls are difficult to keep up to date and can contain names

of people who are no longer legitimate voters. The process is complicated by allowing people to vote at multiple locations, including absentee ballots. The system is probably strongest at protecting ballot secrecy. But, determined poll workers could employ several means to identify the votes of at least some of the voters (e.g., ballot isolation).

Ballot secrecy is an interesting aspect of the system. In many ways, it is the distinguishing feature that makes the process difficult to automate. It is also interesting because in many ways it represents a distinction between a personal issue and a societal issue. A voter can benefit by selling a vote and might not care which candidate is elected. But society faces a huge risk if votes can be sold easily. The important aspect of the manual system is that it does not actually prevent vote selling or coercion. In theory, a candidate could offer money to a voter, and the voter might actually accept the money and cast the corresponding vote. However, the secrecy of the result prevents the vote buyer from determining the true vote. Note that absentee (postal) ballots have been criticized by several people because the secrecy is more easily compromised (both by the individual and by the local election officials).

Cryptographic Tools

Several cryptographic tools have been created to protect transactions. The most common method is dual-key encryption or public-key infrastructure (PKI). This technology is built into Web browsers and used in many situations. It has been in use for many years and proven effective. It has two strengths: (1) It protects any message from interception or modification between the point of encryption and decryption, and (2) It authenticates the computer server (key issuer) to the client computer (browser).

Another powerful cryptographic tool is homomorphic encryption. Cohen and Fischer (1985) explained how it can be used to obscure individual votes without compromising the overall total. Benaloh and Yung (1986) developed a similar process and other researchers have expanded the ideas and methods. The most important feature of homomorphic encryption is that:

$Decrypt_{sk}[Encrypt_{pk}(v_1) *\ldots* Encrypt_{pk}(v_n)] = v_1 + \ldots + v_n$

Each vote (v_i) is encrypted with a public key and stored on a central server. The trick is that the individual votes are not decrypted. Instead, the encrypted values are multiplied together and the result is decrypted. This result contains the same value as the original sum of the raw votes. Adida and Rivest (2006) point out that the Paillier (1999) encryption methodology is particularly effective and it adds a random element to every encryption so that no one can observe the final vote. The encrypted votes can be further protected by using a key-generation system that shares the secret key among several officials.

Homomorphic encryption does add an important risk. If one voter submits an invalidly encrypted vote, multiplying this bad value into the others will destroy the vote. Consequently, another cryptographic tool was introduced, e.g., by Benaloh and Yung (1986). The non-interactive zero-knowledge proof (NIZK) solves the problem because each voter provides a mathematical proof that the data was encrypted correctly and that the result contains only one vote per contest. The zero knowledge aspect of the proof is that the accuracy is shown without revealing the specific vote. For example, Neff (2001) presents a shuffling technique to verify the overall ballot without revealing the individual choices. The non-interactive part of the name stems from the fact that a Fiat and Shamir (1987) heuristic is applied during the process using a shared random string instead of asking for a response from the user (voter). Details were first defined by Blum et al. (1988).

Adida and Rivest (2006) present one of the more complete and interesting uses of these technologies. The primary goal of the approach is the ability to provide an anonymous receipt to the voter. The voter would later be able to verify that the vote posted online matches the receipt—without revealing the actual candidates because of the randomization. With these tools, votes can be submitted securely, counted without revealing the original vote, and provide a means for voters to verify their votes were submitted correctly. Figure 3 shows a sample ballot, where the voter sees the candidate list, but only the matching encrypted value is submitted to the vote-counting server. Each value includes a random element and is submitted with an NIZK proof of correctness.

Candidate d	○ r1
Candidate c	● r2
Candidate a	○ r3
Candidate b	○ r4
Random ordering of candidates	*Server homomorphic-encrypted values submitted as votes*

Figure 3: Ballot with encrypted values

Another Proposal for an Internet-Based Voting System

Although cryptography solves many of the big problems, the critics are correct. Substantial risks remain within the existing proposals. However, it is possible to overcome these risks without too much additional effort. But, the solution does require a couple of twists that are detailed in this section.

Allowing people to vote from personal computers that are potentially insecure causes three serious issues. (1) A voter's computer could contain sophisticated malware that effectively intercepts the communication between the user and the voting system. This software could cause problems in two ways: (a) It could immediately alter the person's vote and hide the actions from the voter. (b) It could capture the voter's credentials and forward them to a third party. (2) Another major challenge is that attackers could mount a denial of service (DOS) attack against the government election servers—preventing people from voting at all. (3) The issue of ballot secrecy is also more challenging when users no longer vote in a public location. In particular, several writers have suggested that coercion (and vote buying) would become possible with an Internet-based (or postal-based) system. All of these criticisms are valid with the systems that have been proposed to date.

Proposed Protocol

The proposed process outlined here is shown in Figure 4 and explained in more detail in the following subsections.

(1) Voters register—possibly manually using existing methods.
(2) Election officials set up a Web site, probably with servers in multiple locations.
(3) Election officials generate public/private keys and publish the public key certificate.
(4) Election officials certify candidates.
(5) Near the election time, the system generates credentials for voters and sends them separately via secondary channels (e.g., postal mail).
(6) The election server generates ballots, with random ordering and an encoded order, similar to the Scratch and Vote protocol, but the ballots are electronic.
(7) Voter randomly chooses or is randomly assigned a ballot, and selects the desired candidates. Only the pre-encrypted vote selection is sent to the election server, not the candidate names. The submitted encrypted votes are validated but not revealed via the non-interactive zero-knowledge proof.
(8) The election process runs for several days, and voters can cast new votes—with only the latest votes being counted. The ending time period would be specified in general, but the exact time would be random, and could be extended in the event of major failures or attacks.
(9) Election officials combine their secret keys and decrypt the vote total, but not the individual votes.

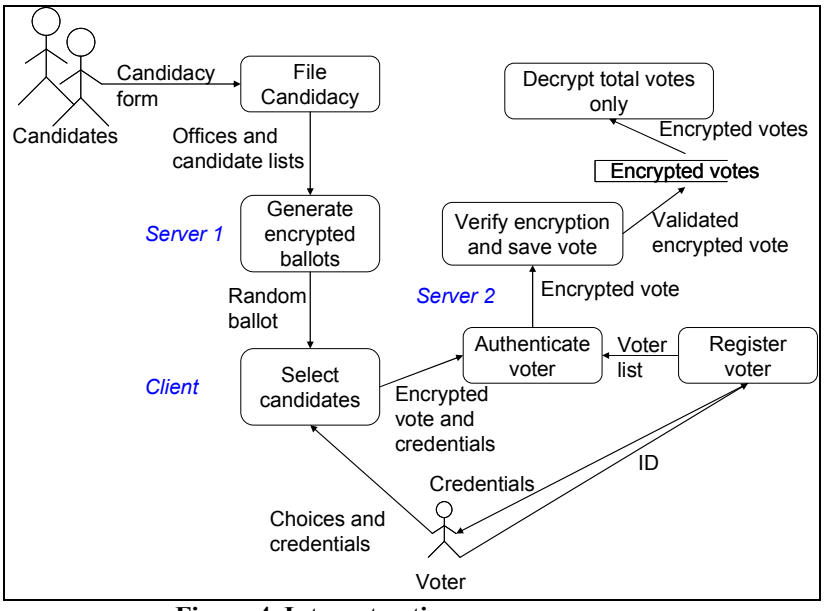

Figure 4. Internet voting process.

The Coercion Problem

The issue in coercion is to prevent the coercer from verifying the actual vote cast. With a relatively long voting period and the ability to recast a vote, the coercer cannot learn the final vote cast. If a coercer paid for a vote and watched the voter cast it, the voter could simply vote again and replace the vote. If a voter sells his or her credentials, the buyer has no way of guaranteeing that the purchased vote will be the final vote cast. The random ending time prevents someone from waiting until the last possible second to cast thousands of collected votes.

However, as pointed out by Kiayias and Yung (2002), all voting systems exhibit some tradeoffs. In particular, "perfect" ballot secrecy is generally sacrificed. In this case, it is not possible to guarantee that the government-run servers provide perfect secrecy. For example, corrupt officials or programmers could use IP addresses to match distributed ballots to votes cast. The risk can be minimized, but it cannot be eliminated. However, that same problem arises with the existing voting protocols. With the Internet system, the voter authentication is separated from the individual ballot—similar to the way voters currently are authenticated separately from the cast vote in today's systems. The voter retrieves a random ballot from one server, authenticates to a second server where only the encrypted vote is cast.

The Denial of Service Problem

Spreading the voting period across a longer time frame also solves the denial of service problem. Using multiple servers in multiple locations also reduces the problem. It would be extraordinarily difficult for an attacker to shut down thousands of servers in different locations for multiple days. Such an attack would cripple the entire Internet—which would give authorities the opportunity to extend the election until the attacks have been reduced to manageable levels.

The problem is slightly trickier if an attacker goes after a limited number of locations. For example, certain U.S. precincts are well-known for voting in specific patterns—largely by political party. An attack on targeted locations might be enough to alter some election results. But, because the election is originally scheduled to run over several days (or even weeks), it would be difficult for attackers to maintain an attack for the entire time. An attack might concentrate on the predicted end of the voting, but election officials could always extend the voting time. Voters should be encouraged to vote early to reduce this risk.

The Spyware or Man-in-the-Middle Attack

One of the most common criticisms voiced against Internet voting is the potential for spyware or Trojan Horse programs to infect voter's computers. These programs could do almost anything—alter a vote and hide the changes from the voter, delete or not submit a vote, or send voter credentials to an attacker. Society cannot guarantee that an individual has a clean computer so critics have condemned Internet voting. However, perhaps the problem is not as large as it appears, and perhaps it is not society's problem. Voters would not be forced to use Internet voting, it would simply be an alternative. Voters who are more competent and willing to trust their computers would be more likely to use the Internet to vote. Additionally, individuals have incentives to keep their machines clean, because they run a far greater risk of losing money. The loss of money is of substantially higher value to the individual than the loss of a vote, so individuals have an incentive to protect and clean their own computers.

In addition, the proposed system presents another way to minimize potential damage from a spyware attack. Voters can vote multiple times and they can vote on different computers. If they suspect that a computer is infected, they can use another computer in a different location. Using the homomorphic approach, the server can display the voter's prior selections. Although these choices are not associated with the candidate list, the voter can verify that at least the positional data was transmitted correctly. An insecure voter could even print out the original ballot choices and compare them to the stored values using a second computer from a different location. Even if the second computer is infected, it would not be able to alter the display from the server in exactly the same manner as the original computer, so the user would be able to spot a problem and revote.

Comparison to Existing Systems

No voting system can be guaranteed correct—not even the existing system. Ultimately, the choice of voting system should be up to the voters. If some voters prefer one method and it is not prohibitively expensive to provide it, the informed voters are the ones who should make the final decision.

The proposed Internet system meets or surpasses existing systems. (1) Eligibility and authentication are similar to existing methods. The public voting booth approach uses humans to validate voter credentials, but it is not clear that average humans are good at this task. Stealing voter credentials would not be a very effective threat, because voters can monitor their own votes. If a voter sees that a vote was changed, new credentials could be issued. An attacker might consider waiting until the last possible minute and flooding the election servers with votes from thousands of stolen credentials. But, with a random ending point, the attacker does not know when to issue the changes. And such an attack would be relatively easy to track. Today, millions of people use similar credentials to handle billions of dollars of transactions. Any rational attacker would go after the money instead of the votes.

The bigger problem with authentication is that voters are likely to lose their credentials. The support costs in issuing new credentials could be relatively large at the start. However, as long as traditional voting booths remain in parallel use, voters could always use those, or be charged a fee to replace lost credentials.

(2) Although voters can vote many times, only the last vote will be counted. Once voters are authenticated, the computer system can do a better job than people at maintaining unique records.

(3) Encrypting the votes and verifying the encryption via NIZK proofs helps ensure that votes are recorded correctly. The primary risks to the accuracy are forged ballots or votes altered by spyware in a voter's computer. Ballot forgery can be minimized through encryption or even NIZK proofs. The spyware problem is reduced by letting users see their final votes (in terms of position and encrypted code). By checking the vote on different computers, the voter can verify the accuracy.

(4) Because the votes are encrypted, they cannot be altered. The only way they can be replaced is via an authenticated user, or an attack on the server. Once again, by enabling voters to verify their votes, this risk is substantially lower with the proposed system than with the existing system.

(5) The final total is automatically verified through the homomorphic encryption process. Similar to the Adida and Rivest (2006) process, the counting is essentially a public process. Anyone can compute the encrypted vote total based on the public data. Only the election officials can decrypt the final count, but they could publish a NIZK proof of the correctness. False reporting could only happen if all of the officials are corrupt. A constraint that is far higher than in the existing systems.

(6) Robustness is improved by spreading the election over a period of time and across multiple servers. Existing transaction-processing technology with redundancy and backup is easily sufficient to handle an election. Individuals can always switch to a different client computer in a different location. Widespread loss of electrical power over a major geographical area for an extended period of time could prevent voters from casting a vote. However, election officials could extend the voting time.

(7) Secrecy is not perfect, but it is relatively strong—at least as strong as with the existing system. In both systems, users could sell votes, but there is no way to prove the final vote, so no candidate or group would spend the money or time. There is a potential risk with the proposed system that the government-run servers could track individual voter choices. However, this risk can be minimized through audits and encouraging election officials to report fraud.

(8) Flexibility is far easier to achieve with electronic systems than with the existing systems. By using standard Web browser protocols, most system would be compatible and existing adaptive technologies could be used by voters.

(9) Voting would be more convenient for many people using the Internet. But, the choice would be up to the voter, so offering Internet voting as an option enables the voter to decide which method is most convenient.

(10) The systems are relatively easy to test and every single vote is validated for encryption accuracy. The servers would need to be tested rigorously, but those procedures are well-defined.

(11) Voters would understand the basic process, but it would be difficult to explain the homomorphic encryption principles. Expert cryptographers could inform the public that the methods securely protect and hide the individual votes. Some people will never believe it, but they can always vote through other methods. The actual voting process would be similar to any other voting method.

(12) Cost is difficult to predict. Building the server software and infrastructure would take money and time. However, the technologies are relatively well-known and easy to create. Ultimately, individual precincts would reduce their expenditures on personnel and voting booths. But, the system would likely require federal funding and testing.

Conclusions

Internet voting can be as secure and robust as the existing voting methodologies. In fact, with voter verifiable results and encrypted votes, it can be more secure. The process is more secure than postal absentee ballots. Considerable work has been performed by the cryptographic community to provide tools that make Internet voting possible. Spreading the voting process over multiple days and allowing voters to change their votes (vote early and often) solves many of the remaining issues. In particular, the commonly-cited threats from coercion/vote buying, denial of service, and spyware are virtually eliminated.

One of the important strengths of Internet voting is that it makes it easy to correct problems that arise. With paper ballots, if the user (or the election authorities) spot a problem, it is almost impossible to fix. For instance, if a voter claims a difference between a receipt and a ballot stored on the election server, how would that claim be investigated? Could a vote be changed after the election? Using Internet voting over a longer time period, the voter can easily revote if he or she believes a problem exists.

Some critics have pointed out that not all voters have equal access to computers and the Internet; which might skew election results, making it easier for wealthier people to vote. It is likely that a greater percentage of wealthier people own computers with Internet access. Any conclusions made from that statement remain conjecture at this point. Almost everyone does have access to the Internet through some means. Additionally, everyone could still vote through other processes, including absentee ballots. It is not clear that adding Internet voting as a new channel is de facto discriminatory. And, there is probably no way to prove or reject the hypothesis short of actual elections.

References

Adida, Ben and Ronald L. Rivest, Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting, *WPES'06*, ACM, October 30, 2006, 29-39.

Association for Computing Machinery, *ACM Policy Recommendations on Electronic Voting Systems*, September 2004, see http://www.acm.org/usacm/Issues/EVoting.htm.

Benaloh, Josh and Moti Yung, Distributing the Power of Government to Enhance the Power of Voters, In *PODC*, ACM, 1986, 52-62.

Blum, Manuel, Paul Feldman, and Silvio Micali, Non-interactive Zero-Knowledge and its Applications (extended abstract), in *STOC*, ACM, 1988, 103-112.

California Internet Voting Task Force (California Secretary of State), *A Report on the Feasibility of Internet Voting*, January 2000, See http://www.ss.ca.gov/executive/ivote/.

Cohen, Josh D. and Michael J. Fischer, A Robust and Verifiable Cryptographically Secure Election Scheme, *FOCS*, IEEE Computer Society, 1985, 372-382.

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, September 2006, working paper, see http://itpolicy.princeton.edu/voting.

Felten, Edward W., Testimony before the Committee on House Administration, September 28, 2006.

Fiat, A. and A. Shamir, How to Prove Yourself: Practical Solutions to to Identifiation and Signature Problems, in *CRYPTO Lecture Notes in Computer Science* vol. 263, Spring 1987, 196-189.

Garamone, Jim, Pentagon Decides Against Internet Voting This Year, American Forces Information Service, February 6, 2004; see http://www.defenselink.mil/news/Feb2004/n02062004_200402063.html.

Help America Vote Act of 2002 (HAVA), Public Law No. 107-252, 116 Stat. 1666, available at http://www.fec.gov/hava/law_ext.txt.

Internet Policy Institute, Report of the National Workshop on Internet Voting: Issues and Research, March 2001.

Jefferson, David, Aviel D. Rubin, Barbara Simons, and David Wagner, Analyzing Internet Voting Security, *Communications of the ACM*, October 2004, 47(10), 59-64.

Kiayias, Aggelos and Moti Yung, Self-Tallying Elections and Perfect Ballot Secrecy, *Proceedings of Public Key Cryptography, PKC*, in *Lecture Notes in Computer Science* 2274, Spring 2002, 141-158.

Mercuri, Rebecca T., *Electronic Vote Tabulation: Checks and Balances*. Ph.D. thesis, University of Pennsylvania, 2001.

Mercuri, Rebecca T. and L. Jean Camp, The Code of Elections, *Communications of the ACM*, October 2004, 47(10), 53-57.

Mohen, Joe and Julia Glidden, The Case for Internet Voting, *Communications of the ACM*, January 2001, 44(1), 72-85.

Neff, C. Andrew, A Verifiable Secret Shuffle and its Application to e-Voting, In *ACM Conference on Computer and Communications Security*, ACM, 2001, 116-125.

Paillier, Pascal, Public-key Cryptosystems Based on Composite Degree Residuosity Classes, in *EUROCYRPT*, 1999, *Lecture Notes in Computer Science*, vol. 1592, ed. J. Stern, Springer 1999.

Phillips, Deborah M. and Hans A. Von Spakovsky, Gauging the Risks of Internet Elections, *Communications of the ACM*, January 2001, 44(1), 73-85.

Shocket, Peter A., Neil R. Heighberger, and Clyde Brown, The Effect of Voting Technology on Voting Behavior in a Simulated Multi-Candidate City Council Election: A Political Experiment of Ballot Transparency, *The Western Political Quarterly*, June 1992, 45(2), 521-537.

Stromer-Galley, Jennifer, Voting and the Public Sphere: Conversations on Internet Voting, *PS: Political Science and Politics*, October 2003, 36(4), 727-731.

Williams, Brit J. and Merle S. King, Implementing Voting Systems: The Georgia Method," *Communications of the ACM*, October 2004, 47(10), 39-42.

Xenakis, Alexandros and Ann Macintosh, ICEC 2004, Proceedings, *Sixth International Conference on Electronic Commerce* (ACM), 2004, 541-546.

ZDNet, Government Blog, December 21, 2006, at http://government.zdnet.com/?p=2789.