Electronic Voting as the Key to Ballot Reform

Rick Gibson
American University, USA

Christopher Brown
American University, USA

BACKGROUND

The emergence of online markets and e-business was expected to revolutionize market structures, supply chains, and consumer behavior. The technological potential led to hasty forecasts that predicted extremely low costs for information. Corresponding communications advances suggested increased transparency and response speeds. Nowhere have these expectations been shown to be more flawed than in the attempted application of electronic voting in the United States. Following the controversy of voting fraud accusations, such as the narrow margin in the Florida election counts in 2000, traditional voting methods have suffered a general loss of trust in the public perception (Dill et al., 2003). These methods, which include but are not limited to optical readers and punch-card ballots, have been heavily scrutinized by critics in the wake of reports of widespread malfunctions, which suggest that the primary attributes of a successful e-vote scheme: anonymity, scalability, speed, audit, and accuracy. It also brings much criticism into the picture in regard to the reliability of direct recording electronic (DRE) voting machines.

Cranor (2001) reported that, in Florida, esoteric terms for voting mishaps (e.g., the "hanging chad") became the focus of many postelection jokes due to faulty punch-card machinery. Moreover, she reported that some local polling sites in New York with ancient voting mechanisms were missing levers. These machines had been manufactured so long ago that the necessary maintenance could no longer be performed. Such technical problems present huge obstacles for vote integrity.

Weiss (2001) provided explanations of the many ways in which votes are recorded and how effective (or ineffective) these methods have been in elections. The author provides a general overview of the possibilities for Internet voting in addition to drawing a parallel between it and ATM transactions, noting the importance of setting up an e-vote system, which takes advantage of the same kind of transaction-based technology as ATMs, which do not use the Internet per se—thus dealing with the social issues that often go hand-in-hand with a fundamentally new advance in voting procedure, such as the conveto the aforementioned faulty voting machines, there is a real concern regarding ballot design in light of "butterfly ballot" confusion made notorious during the Florida national election. Such odd designs are the result of election officials putting the function of the voting machine ahead of voter readability and understanding. Thus, even voters with 20/20 vision and great hand-eye coordination may not be able to vote properly with poor ballot layouts, contrary to the popular belief that such voting errors resulted from those voters of old age with visual handicaps. Mercuri (2002) reported on the defects of DREs brought into Florida poll sites after the election fiasco of 2000. New technologies should be studied further until real implementation can be brought into the polling sites.

If U.S. citizens look beyond their own national issues with voting failure, they find themselves behind the times when they glance at other democratic countries such as Brazil and Costa Rica (Weiss, 2001). Such systems involving secure electronic implementations force voters to consider the benefits of electronic over paper systems in terms of voter fraud, cost, accessibility, and usability.

One pertinent question becomes obvious at this point: Why are poll sites continuing to use voting equipment that does not meet the needs of its voters? If the mechanisms for voting are compromised, the very nature of our democracy is threatened. Undoubtedly, as with any information system, the success of the electronic voting process critically depends on voters' beliefs and feelings about the electronic voting process. The more voters, become aware of the system's failure and lack of credibility, there will be less trust in the efficacy of the voting procedures and in those who oversee elections.

As a response to the degeneration of traditional voting methods and spurred by technological paradigms, *e-voting* has become a new catch-phrase in ballot reform. This new term, however, is shrouded in ambiguity. On one side of the debate we have those that talk about e-voting in terms of the Internet and the ability to cast votes from a great number of different locations (Weiss, 2001). The other camp of e-voting still thinks of the process in the traditional sense of conducting elections at local polling

sites, but instead polling sites would be virtually, if not entirely, paperless. Both camps, however, agree that e-voting has the potential for solving the problems of traditional voting techniques but must first be approached with cautious planning.

DESCRIPTION OF E-VOTING ISSUES AND ALTERNATIVES

Internet voting takes advantage of remote access to increase voter participation. This follows from the logic that most people are familiar with browsing the Web from their personal computers and will more readily be able to participate in an election where both physical and scheduling obstacles do not interfere. Mohen and Glidden (2001) described how the 2000 Democratic primary in the state of Arizona utilized the power of Internet voting in conjunction with mail-in and poll-site options. The voting process, run through election.com, enabled Democrats from all locations within the state to vote on their personal computers with Internet access. Voter identity and authentication were successfully dealt with in a secure operating environment. Internet voting advocates in the state claim that polling site locations were increased in those areas that had limited access. They present the Arizona Democratic primaries as a success in e-voting and a fundamental reason for encouraging states to adopt such e-vote measures and also show the decryption technologies available for use and the effectiveness of these techniques for combating hackers.

Although groups like the Voting Integrity project have taken issue with Arizona's implementation of Internet voting in regard to its exclusion of those minority voters without Internet access (Craft, 2000). In addition to the Arizona primary in 2000, the Alaskan Republican Party's presidential straw poll utilized the Internet for voting in January of the same year. In this example, geographically inaccessible polling sites and other physical limitations could only be overcome by using a quick and easy remote access method. Craft (2000) also provides an overview of some case-studies in Internet voting and the pitfalls that it might succumb in terms of security. Specifically, the voices of the California Internet Voting Initiative are heard in regard to what we would need to do in order to preserve the integrity of elections.

Following from this, we also see the benefits for U.S. citizens currently involved in overseas military action or for a number of personal reasons, as opposed to mail-in ballots. To support this move, researchers have discovered that mail-in fraud had been on the rise since states have become less strict with the procedural rules (Phillips & von Spakovsky, 2001).

Rubin (2002) asserted that the major concern of such remote voting techniques lies within the realm of security, especially when one considers the possible manipulation of votes by hackers or denial-of-service attacks on Web servers hosting these election sites. Such a large-scale implementation of Internet-based voting could seriously compromise the nature of an election by a concerted effort by malicious online entities. He delves into the concerns over security breaches to a communications infrastructure supporting an online election system. Thus, social engineering, in addition to technical hacker attacks, is a threat lurking beneath the obvious ways of manipulation. For example, pseudoelection servers could be set up on the Internet to trick those unfamiliar with e-voting into believing they have actually cast a vote when they have not. There must be secure voting in order to ensure votes are not "stolen" by malicious hackers.

E-voting advocates, however, do not always support the Internet voting method. On the other hand, some advocates say traditional polling sites should convert the mix of old voting methods (such as paper ballots, punch-card ballots, optical-reader ballots, and lever ballots) to an electronic medium. A private network, as opposed to the public Internet voting framework, provides a safer, more secure transmission of ballot choices. Such a network depends on direct recording electronic systems (DREs) to present information to each voter in a way that is easy to read and understand and capable of accurately and reliably recording voter choices to a back-end database server.

Proponents of these machines often refer back to the not-so-distant past with regard to the butterfly ballot scandal in Florida. Better prepared visual layouts are promised through the use of electronic interfaces, in which the function of the device does not determine the layout. Whether or not this actually occurs in practice within the DRE market is questioned by analysts, such as Bederson et al. (2003), who further consider how malicious coding by private e-vote companies (unregulated) can corrupt election results. This leads to the question of the design of e-voting systems, such as Diebold AccuVote, and their accessibility, including ballot layout issues and their impact on elections, in addition to the problem of training requirements for both election site officials and voters.

In both forms of e-voting there is the primary concern of being able to recount votes and analyze the paper trail for corruption. Whether this serves merely the losing candidate's political vested interests or the will of the people, however, is questionable. It is clear, however, that some alternative auditing techniques must exist for the voting system to have validity within the eyes of the voters involved in the entire process. Zetter (2004) illus-