EDITORIAL PREFACE

Preventing E-Voting Hazards: The Role of Information Professionals

Jo Ann Oravec, University of Wisconsin, USA

ABSTRACT

In its ideal form, electronic democracy would empower citizens to vote online with convenience, security, reliability, and accessibility. However, electronic vote fraud can prevent citizens from exercising their basic rights in a democracy. Inaccessible e-voting systems also can deny citizens their rights. Unfortunately, attention to these problems generally is muted in the popular media, as those concerned are being accused of spreading rumors and conspiracy theories. This article explores how information technology professionals can employ their expertise to play important roles in dealing with these critical issues.

INTRODUCTION

Citizens cast votes in the U.S. only a few times a year (at most). Between elections, few of them may stop to think about the systems through which their votes are tabulated. How do they know that the votes they cast will be counted fairly and accurately when the next election rolls around? This question is critical to basic civic functioning in many nations. However, the introduction of advanced information technologies into the voting process has stimulated complex concerns at nearly every stage (Fund, 2004). For example, the increasingly widespread use of touchscreen machines (often without paper trails) has popularized such disturbing phrases as black box voting and vote scam (Collier & Collier, 1992; Harris, 2004). The kinds of oversight that have been given to elections in generations past are becoming ineffective rapidly since e-voting systems have the potential for manipulations that are imperceptible to all but the most skilled computer forensic experts (Lauer, 2004).

Vote fraud has been a fact of life for as long as voting itself has been in existence. However, e-voting issues engender a new assortment of potential technological concerns, both ones that are due strictly to flaws in the technology and those that are linked to partisan tinkering. Concerns with the security and reliability of voting systems should be opened to public examination well before elections are conducted to ensure that preventive measures are taken if possible. After elections, discussion is critical as well — although non-
partisan discourse is often more difficult at that point. However, valid objections to unfair or apparently faulty electoral practices should not be disregarded in the quest to create the facade of fair elections or support the objectives of governmental efficiency.

The introduction of advanced information technologies into vote fraud and suppression issues has added additional, complex factors to discourse on voting. Information technology professionals are familiar with basic security concepts (as well as with notions such as source code) and can serve as resources to citizens and public administrators when issues arise. Supplying the technological infrastructure for elections has become a profitable business, with corporations competing for available taxpayer dollars and fears of partisanship emerging (Thompson, 2002; Harris, 2004). Information technology professionals have much experience in dealing with such corporations, and may be best equipped to advise public officials in these areas. Since corporations can change in political allegiance and new players can enter the computer voting industries rapidly, it is in the best interest of members of all parties to be vigilant in these matters. Everyone has an interest in maintaining a system of fair and open elections.

In the U.S., the more traditional media (e.g., television and print newspapers) have provided only minimal coverage of e-voting issues. The relative lack of press coverage may be surprising, given the importance of having a strong and secure voting system. Internet-based voting problems associated with such television programs as American Idol have garnered considerable amounts of attention in the national press. A number of nationally-syndicated stories alarmed readers with the possibility that the person chosen as the best performer in the show would not be chosen through a fair balloting process. Information technologists can direct the public’s attention to comparable issues that lie ahead for them in their own electoral systems — with far greater stakes at risk.

**PROPOSED SOLUTIONS FOR E-VOTING CONCERNS: PAPER BALLOTS?**

Public awareness of e-voting concerns is just emerging; meanwhile, formidable (and expensive) systems of electronic voting are being put into place. Some of the requirements for these systems in the U.S. were instituted by HAVA (the Help America Vote Act of 2002, Public Law 107-252), which was enacted in part in response to voter distress after the 2000 presidential election. The Act called for the streamlining of voting systems but did little to prevent the control of the systems by such corporations as Diebold, ES&S, and Sequoia; thus, it has raised concerns by those of various political affiliations (Fund, 2004; Harris, 2004). One of the major problems with high levels of corporate control of various stages in the voting process is that trade secrets often are kept from the public through contractual means. The source code programming for the systems — which would give governmental or other outside inspectors the potential to determine potential bias — generally is not released. In
contrast, in the Netherlands, the code involved is open source and available to all (Libbenga, 2004). Some of the systems used in the 2004 U.S. presidential election did not have a paper trail, so the issue of a recount was muddy conceptually. Prospects for the privatization of voting systems are quite alarming given the potential negative side-effects of direct corporate intervention in politics.

Ideally, computers would be solving problems of voting systems rather than causing them: Electronic enhancements to voting systems are reportedly ways to bolster the systems’ integrity, not undermine it. However, there are many new insecurities related to e-voting. As a historian reflected after the 2004 election:

*In many areas of the country, vote buying, ballot-box stuffing, voter suppression and intimidation, even outright thievery have long been components of the political culture, and voters have had to rely on little more than blind faith in hoping that their votes would be accurately assigned to their chosen candidates. As the angry accusations fly in late 2004, where do we stand historically? Are you better off than you were 4, 40, or 100 years ago?* (Campbell, 2004, p. B11)

Paper back-ups for touchscreen votes have been projected as at least one way that the most egregious kinds of e-voting fraud can be avoided (Fund, 2004). Those who demand paper ballots, or at least a paper back-up, often have been dismissed as Luddites (i.e., individuals who oppose technology, based on irrational fears). A Christian Science Monitor story took these fears seriously, however:

*Imagine your bank teller accepting a deposit and then saying, “Oh, you don’t need a receipt. It’s all in the computer.” On Nov. 2, that’s essentially what millions of citizens will be told when they cast ballots on new electronic voting machines. Forty-two states are poised to use this latest technology, but with only 28 days left until the presidential election, some states are still debating whether to provide a paper confirmation of each voter’s choices.* (Leach, 2004, p. 11)

Such a paper trail indeed may add to the expense of elections but it could help in lending them credibility. Information technology professionals are needed not only to design these systems but also to educate both citizens and public officials on these matters.

**SOME CONCLUSIONS AND REFLECTIONS**

Vote fraud is a very severe way of silencing citizens’ voices. Elections currently are conducted within certain windows of time, so temporal considerations are paramount in dealing with problems as they emerge. Voting difficulties certainly can inspire cynicism, as expressed in this comment after the 2004 State of Washington gubernatorial vote recount:

*State Republican Party Chairman Chris Vance says he can’t decide whether Democrat officials in heavily Democratic King County — where uncounted or improperly discarded ballots keep popping up — are “colossal incompetent or completely corrupt.”* (Hallow, 2004)

Citizens need straightforward information about the potentials for e-voting
fraud, as well as specific ways in which to be proactive about these issues. Information technologists, in their roles as experts, can help citizens explore how their own states and localities integrate electronic machines into their voting systems. They also can work with officials in designing plans for future technological initiatives. Nationwide discourse, informed by experts, is needed to sort out these difficult issues and develop workable solutions. These are complex matters that are comparable in many ways to other public policy concerns dealing with black box high technology, in which the complexity of the system impedes external analysis by its everyday users (Oravec, 1996). Information technology professionals can work to protect their own rights to vote as well as aid in designing more accessible and user-friendly voting systems. With the myriad of changes in vote-processing techniques associated with computing, all citizens need to be aware of possible obstacles to a fair electoral process.

REFERENCES


Jo Ann Oravec (MBA, MA, MS, PhD) is an associate professor in the College of Business and Economics at the University of Wisconsin at Whitewater (USA). She chaired the Privacy Council of the State of Wisconsin, the nation’s first state-level council dealing with information technology and privacy issues, and has written several books. In 2005, she will be a visiting fellow at Cambridge University.