IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4755

I-Voting: To have or not to have?

Trisha Woolley and Craig Fisher, Ph.D.
Information Systems
Marist College
Route 9
Poughkeepsie, NY 12601
TrishaWoolley@cs.com, Craig.Fisher@Marist.edu

ABSTRACT

This paper discusses issues relating to the use of Internet Voting (I-Voting) in public elections. We found that the United States is not ready to accurately count votes electronically. Information systems are currently inadequate to deliver a socially responsible voting system. However several pilot voting projects provide hope.

INTRODUCTION

One would think that by the 21st Century the most technologically advanced country in the world would be able to accurately count votes. However the Florida 2000 election has lead to outrage at the lack of ability to simply count votes. "An entire nation shared in a bug reporting exercise that will likely accelerate fundamental changes to how we administer democracy in the near future" (Weiss, 2001).

Currently, voting takes place at supervised local polling sites with largely antiquated polling machines. Due to the recent popularity of e-commerce many are asking whether the voting process should take place electronically through the use of the Internet. Internet voting [or I-voting] promises to solve several social problems. An individual could vote from his/her home or office rendering obstacles such as traffic, weather and working hours irrelevant. Disabled people and "shut-ins" could have easy access to voting systems (Sink, 2000). In addition, since computers can accurately and rapidly tabulate millions of financial transactions daily, the public naturally believes that I-voting may improve the accuracy of elections (Gugliotti, 2001), may increase voter turnout and are more secure than punch card systems (Raney, 1999).

I-voting departs from traditional voting techniques in that it uses computers that are "not necessarily owned and operated by election personal " (California Internet Voting Task Force (CIVTF), 2000). This supervision is a cornerstone of our election process and to maintain principles of secret ballots and free elections, the United States government must approve all election equipment and procedures.

While I-voting is not yet approved for usage as election equipment, it is being tested and observed in distinct elections. Pennsylvania's Montgomery County has moved from mechanical to I-voting, replacing its 40-year-old voting booths with new MicroVote machines in 1992. The March 2000 Arizona Democratic Party is the first time I-voting was used in a presidential preference primary (Mohen and Glidden, 2001). The U. S. Military staged a pilot (Phillips and Von Spakovsky, 2001) that illustrated that people can vote over the Internet under ideal conditions. However it contained only 250 voters and most conditions are far from ideal.

This paper reviews the issues and concludes that our nation is not yet ready for I-voting. I-Voting technical issues include security, authentication, privacy, access, and data quality. However, the many advantages of I-voting should not be lost and therefore we recommend an increase of local elections performed through the Internet to gain knowledge and experience.

SECURITY

Voting fraud is very real in any election, for example, "the 1997 Miami mayor's race was thrown out due to massive absentee ballot fraud" (Phillips and Von Spakovsky, 2001). A secure system "is one that can withstand attack when its architecture (cryptography, firewalls, locks, etc.) is publicly known" (Rothke, 2001). Typically, systems use simple user-ids and passwords but these are considered risky because hackers can use software tools to discover most passwords (Rothke, 2001).

Some say that I-voting systems are more secure than punch card systems that require human intervention (Raney, 1999). The overlapping of several applications increases security as in the case of the Arizona democratic election where system layers of user interface, business logic, and database access, combined with a third party count, adequately secured the votes (Mohen and Glidden, 2001). Independent review by knowledgeable experts and public observers is essential (Phillips and Von Spakovsky, 2001).

However viruses and denial of service attacks are easier to perform in the Internet environment than with traditional voting methods (Phillips and Von Spakovsky, 2001). Threats to host computers have higher risk, are more detrimental in their outcome and are harder to detect than conventional threats. They are high risk because large numbers of votes could be manipulated at once without being detected (Mohen and Glidden, 2001). The distributed nature of I-voting makes it difficult to establish tampering patterns that are detectable (Weiss, 2001).

Threats to the Internet are compounded by the millions of novices who would be required to use the system (Phillips and Von Spakovsky, 2001) and poorly designed interfaces (Weiss, 2001). I-voting requires an infrastructure where 200 million people could vote on a single day but no such system has yet been implemented. Some popular electronic funds transfer systems can only perform that many transactions per day not per hour. (Rothke, 2001) The combination of workload, inexperience and a new technology will result in a negative outcome.

AUTHENTICATION

Vote selling is viewed as a major threat to I-voting. Large groups of voters may gladly sell their votes to the highest bidder if an Internet system is invoked and if there is no way to authenticate the voter. More sophisticated Identification such as retina recognition is required by an I-voting system to verify both the identity and eligibility of potential voters but identification software is not yet accessible to all voters (CIVTF, 2000). In addition today's machines don't offer options that would prevent accidental voting for the wrong candidate (Weiss, 2001; Schwartz, 2000).

ACCESS

Access to I-voting does not necessarily lead to increased voter turnout but I-voting could be seen as a barrier. People are more likely not to vote due to apathy rather than because they cannot use their PCs (Ritchie, 2002). However barriers to access could lead to a decrease in voter turnout. When voting from home, voters face a potential barrier to access if their computer breaks down or there is a loss of electricity. During the Arizona election, a "one hour outage occurred due to a hardware failure in a router" (Mohen and Glidden, 2001).

Another barrier to access would include Denial of Service (DOS) in which a hacker floods the Internet during an election. In the Arizona Democratic primary the voting system deflected several DOS's. "Intrusion-detection software monitored activity on the voting network, de-

tecting when unusual activity occurred and filtering it out, thus preventing it from interfering with the servers. We also configured the system's firewalls and external routers to minimize the effect of a distributed DOS attack" (Mohen and Glidden, 2001).

DATA QUALITY

A quality I-voting system depends upon the accuracy of the database of registration records (Phillips and Von Spakovsky, 2001) and a reliable secure workstation-network infrastructure. A voting system is accurate if (1) it is not possible for a vote to be altered, (2) it is not possible for a validated vote to be dropped, and (3) it is not possible for an invalid vote to be counted in the final tally (Cranor, 1996).

With the inaccuracies of the Florida 2000 election vote count, it is realized that the voting machines are not error-proof and a new technology needs to be developed to increase the accuracy of the count of votes. "Voters who used out-dated punch card machines were 7 times more likely to have their ballots discarded. But when minority voters had access to better technology, their votes were more accurately counted" (Kennard, 2002).

Computers offer the opportunity to provide an interface that is tightly controlled, has less human intervention, more accuracy of voting tabulation, and improved timeliness (Gaboury, 2002). In addition the Internet could maintain voter registration information produce more accurate voter rolls (White, 2001)

DIGITAL DIVIDE

The *Digital Divide* is "defined as those who have Internet access from home or work and those who don't" (USA today). The voting rights act of 1965 states that every voter has to have equal access to a computer and an equal right to vote, which is not the case. The *Digital Divide* is a challenge to I-voting because of the wide differences of availability of I-access based on demographics such as age, income, education, region, occupation and ethnicity. Only half of Americans have Internet access (USA Today).

On the "have" side of the divide are those with higher income (Novak and Hoffman, 1998; Kennard, 2002), higher education (Novak and Hoffman), being white (Phillips and Von Spakovsky, 2001), being younger (CIVTF, 2000), and those living in the Western region of the U. S. (CIVTF, 2000). Nationally, as of December 1998, only 19% of African Americans and 16% of Hispanics had Internet access from any location, compared to 38% of whites. African-American and Hispanic households are only 40% as likely as white households to have home Internet access (Phillips and Von Spakovsky, 2001).

An analogy may demonstrate the significance of the *digital divide*. If public officials announced that they were going to add five more polling places within an all white neighborhood there would be outrage due to the inequity. But I-voting does just that – it puts a polling place in everyone's home who has I-access – just shown to be the "haves." (Phillips and Von Spakovsky, 2001).

VOTER PRIVACY

Privacy is one of the most important aspects of voting for elections (Mohen and Glidden, 2001) but I-voting does not give voters enough privacy (Larsen, 1999). Family members and friends may be privy to personal identifiers needed to 'secure' online voting and could either coerce or simply vote in place of individuals. Network administrators using their networked office computers could change ballots. I-voting might encourage organized voter coercion by groups such as employers, churches, union bosses, nursing home administrator, and others (Phillips and Von Spakovsky, 2001)

The "opportunity to approach a voter with a baseball bat, buying and selling votes, especially from the apathetic, greedy, or poor" is increased with I-voting (Weiss, 2001).

PEOPLE WITH DISABILITIES

I-voting can accommodate the disabled people to cast votes (Mohen and Glidden, 2001). The computer interface can allow for several different fonts, prints, and sizes to accommodate different voters. For example, larger font size can aid the visually impaired. Customizable interface and Internet access to the home will give disabled voters increased access to the voting process (CIVTF, 2000). However this potential is not always realized as in the Arizona primary election where auditory prompts were omitted, greatly hindering blind voters (Phillips and Von Spakovsky, 2001).

PUBLIC CONFIDENCE

The public must feel comfortable with the security, results, and outcomes in order to trust the technology (CIVTF, 2000). 63% of adults currently oppose I-voting due to uncertainty of cyberspace (Phillips and Von Spakovsky, 2001). Many pilot tests involving thousands of people are needed prior to conducting an election with over 200 million voters.

In November 2000, voters in San Diego and Sacramento counties were able to try online voting from computers at polling places. The test was conducted for the state by VoteHere.net, which ran similar trial in Maricopa County, Arizona. The company released polling results after the vote suggesting that "100% of voters who used the system found it easy to use, that 80% said they preferred I-voting to the current system, and that 65% said they would vote from home if they thought the system was secure." (Schwartz, 2000).

However, if there are technological errors, there will be long lines, voter frustration, and loss of confidence in the election process. For example, during the Arizona 2000 presidential primary, "The Internet Corporation for Assigned Names and Numbers (ICANN) board suffered from voter registration problems as well as overloaded servers that caused many voters to be turned away from the voting Web site" (Mohen and Glidden, 2001).

MEDIA

Internet elections will "generate an enormous media interest." (Phillips and Von Spakovsky, 2001) "Any real or perceived threat to a voter's privacy will probably lead to extensive negative publicity...When the technology driving teledemocracy fails, it is hard or impossible to cover it up. Such failures are widely publicized. The Monroe case was highly publicized for its failures...Even sub percentage failure rates may affect the votes of thousands of people. Such errors may, in addition to receiving much attention from the press, leave potential voters disillusioned about their role in our democracy" (Larsen, 1999). Also, "it would be difficult to prevent political advertising form appearing on-screen and in the ballot window during voting if the voter's Internet Service Provider is one that displays advertising." (CIVTF, 2000)

LEGAL

State and federal laws are not geared toward governing remote electronic elections and the vendors that run them. There are no laws, standards or requirements for hardware or software. Legally "Internet Voting opportunities must be accessible to all voters, including low income voters whose only access to the Internet may be through public access Internet terminals that are commonly available in libraries and schools. Internet ballots must be available in multiple languages in jurisdictions required to print multi-language ballots to conform to the Federal Voting Rights Act of 1965" (CIVTF, 2000). Rothke (2001) said, "No electronic voting system is certified (even at the lowest level) of the US government . . .." In addition to accessibility requirements, a lack of standards could lead to ballots that are as confusing as the butterfly ballot used in Florida (Rothke, 2001).

ECONOMICAL

It is still not clear if I-voting is economically feasible. There are advantages to I-voting, but there are also disadvantages. The advantages include efficiency of administering elections and counting votes (Rothke, 2001), accuracy and speed of the automated voting system (Schwartz, 2000), availability of information and reduced transaction costs (Watson and Mundy, 2001), reduced number of polling places

needed (Phillips and Von Spakovsky, 2001), and reduced travel expenses (Cranor, 1996).

An I-voting system would require several changes to the current system. This includes the cost of help desk support (Rothke, 2001), education of voters, training of election officials (Cranor, 1996), and reconfiguring of computer systems (CIVTF, 2000).

Since voting is only performed once or twice per year the market for voting software systems is relatively small (CIVTF, 2000). Therefore, election system vendors are forced by competitive bidding pressures to offer the cheapest possible systems with minimal fraud protection (Saltman, 1998).

CONCLUSION

While on the surface, I-voting appeared to be imminent; it now looks like it will be quite some time before we can depend on national elections over the Internet. The benefits, such as increased convenience, accuracy, efficiency, enhanced information and access to the disabled, are outweighed by the negative factors, such as inexperienced vendors, users, and election personnel, the digital divide, no laws for compatibility, privacy issues, and technological issues. Pilot tests should be conducted at local levels to facilitate integration, cooperation, and compatibility of the technologies, vendors, and users.

I-voting requires numerous technical and procedural innovations to ensure accurate voter authentication, ballot secrecy and security. Any socially responsible use of the Internet for voting purposes should be phased in gradually to ensure that election officials and members of the public are experienced, educated and confident with the technology.

The digital divide may always exist but in different forms. At some point all people may have Internet access just like they have the telephone but the quality of access might be different. For example, the digital divide might change to who has broadband versus who uses dial-up access.

REFERENCES

Berghel, Hal. Digital Village: Digital Politics 2000. *Communications of the ACM. Vol. 43.* No. 11. November 2000

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

Cranor, Lorrie F. Electronic Voting: Computerized Polls May Save Money, Protect Privacy. *Crossroads. Vol. 2* No. 4. April 1996.

Does the Internet Represent the Future of Voting? USA Today. Vol. 130. No. 2683. New York. April 2002

Gaboury, Jane. The Mouse That Roars. *IIE Solutions.* Norcross. Vol. 34. Issue 1. January 2002.

Gugliotta, Guy. Study Finds Millions of Votes Lost; Universities Urge Better Technology, Ballot Procedures. *The Washington Post*. Washington, D.C. July 2001.

Kennard, William E. *Democracy's Digital Divide.* Christian Science Monitor. Boston, Massachusetts. March 2002.

Larsen, Kai R.T. Voting Technology Implementation. *Communications of the ACM. Vol. 42* No. 12. December 1999.

Mohen, J., and Glidden, J. The Case for Internet Voting. *Communications of the ACM. Vol. 44.* No.1. January 2001.

Novak, Thomas P., and Hoffman, Donna L. Bridging the Digital Divide: The Impact of Race on Computer Access and Internet Use. Vanderbilt University. February 1998. http://ecommerce.vanderbilt.edu/research/papers/html/manuscripts/race/science.html

Phillips, D.M., and Von Spankovsky, H.A. Guaging the Risks of Internet Elections. *Communications of the ACM. Vol.44.* No.1. January 2001.

Raney, Rebecca. *Casting Ballots Through the Internet.* New York Times. NY May 1999.

Ritchie, Ken. *Letter: A Low Poll for Internet Voting.* The Guardian. Manchester, UK. January 2002.

Rothke, Ben. Don't Stop the Handcount: A Few Problems with Internet Voting. *Computer Security Journal. Vol. 17.* No. 2. Spring 2001.

Saltman, R.G. Accuracy, Integrity, and Security in Computerized Vote-Tallying. *Communications of the ACM. Vol. 31* No. 10. Ocbober 1998.

Schwartz, , John. *E-Voting: Its Day Has Not Come Just Yet.* New York Times. New York, N.Yn. November 2000.

Sink, Mindy. *Electronic Voting Machines Let Disabled Choose in Private.* New York Times, N.Y. November 2000.

Voting Rights Act of 1965 . South Carolina v. Katzenbach appendix. Prentice Hall Documents Library. 1966. http://hcl.chass.ncsu.edu/garson/dye/docs/votrit65.htm

Watson, R.T., and Mundy, B. A Strategic Perspective of Electronic Democracy. *Communications of the ACM. Vol. 44.* No.1 January 2001.

Weiss, Aaron. *Click to Vote.* netWorker. Vol. 5. No. 1 March 2001.

White, Ben. *Internet Voting: A Web of Intrigue?; Study Says There's Too Much Risk.* The Washington Post. Washington, D.C. March 2001.