Internat Voting: Will it Spur or Corrupt Democracy?

Lance J. Hoffman
Computer Science Department
The George Washington University
Washington, D. C. 20052
hoffman@seas.gwu.edu

People have been voting by mail for many years for officers of corporations and on various issues of organizations to which they belong. In recent years, they have been able to cast these votes by the Internet, often using third party suppliers of voting system services. A logical next step, many say, is allowing citizens to vote for public officials over the Internet.

Some Internet Voting Experiments

Some trials have been carried out or proposed to take place in parallel with government-related elections:

- In Alaska in January 2000, 35 people voted via the Internet in the Alaskan Republican Party's presidential straw poll using a password mailed to them in advance[1] . Kathleen Dalton, a member of the Alaska Republican Straw Poll Committee said that "Internet voting opens up a completely new domain to an Alaskan population that is handicapped by vast distances, lack of land transportation routes, and slow or interrupted postal service in winter months".[2]

- The Arizona Democratic Party was planning to offer Internet voting in its March 2000 binding presidential primary. Security in this election appeared also to rely on voters signing a form, mailing it in, and receiving by return mail a password that allows them the vote any time within a four-day period. A firm competing with the one running the election for the party declined to make a bid for the election. They were concerned that party officials insisted on allowing people to vote from home, and urged instead voting only at polling stations, so poll workers could guarantee the identity of voters before letting them cast votes. They also worried that the computers used might harbor viruses or other Trojan horse programs. [3] The Voting Integrity project has filed suit in federal court against the Arizona plan, saying it discriminates against minority voters. [4] Noting that only half of the households in the United States have Internet access, the League of Women Voters has raised this issue also.[5]

- The Pentagon is scheduling a test of overseas Internet voting in November 2000 using 250 voters from five states and virus-free machines.

Promises and Pitfalls

Proponents of Internet voting for government elections point to convenience, 24-hour availability over several days, and the ability of Internet voting to be unaffected by traffic and weather issues. However, "Election Day" for a 17-day period "not tied to a polling place" (by mail) has not increased turnout in Texas[6]. Proponents also claim potential cost savings in the long run. The California Internet Voting Initiative for the November 2000 ballot "requires counties to provide means for Internet registration and for all public electoral jurisdictions to provide means for Internet voting".[7]

Opponents view with alarm the potential vulnerabilities of Internet elections. "An Internet election is going to be a natural target for hackers" says Hans von Spakovsky of the Voting Integrity Project[8]. Governors Gray Davis (of California) and George Pataki (of New York) have noted that the security in voting systems must be greater than that in e-commerce systems which internalize the costs of a relatively minor amount of fraud. Voting systems must have security and integrity at a higher level to insure that elections are not stolen and to maintain public confidence. The governors stress the need for full public debate and testing of any proposed Internet voting system before its use in public elections. [9]

The California Internet Voting Task Force suggested in a January 2000 report[10] that Internet voting be gradually phased in over time, as the technology proves itself: voters first would be allowed to cast ballots on Internet-connected computers at the voter's polling place, then at any polling place in the voter's county, then from county computers or kiosks, and finally from any Internet connection. One major recommendation of the California report is to disallow remote Internet voter registration systems until there are strong online human identification mechanisms widely available, along with ways to verify citizenship, age, and residency. It concluded that the use of digital signatures on initiative, referendum, and recall petitions should be prohibited because of the lack of a standard method of digital identification. Another conclusion was that Internet voting (as opposed to registration) systems "must be divided into two fundamental classes:

> (a) those in which the election officials control the voting infrastructure on the client side, including the client machines, their software, and the LANs they are connected to, and
> (b) those in which the voter or a 3rd party controls the client environment, e.g. voting from PCs at home, office, university, hotel, etc.

"Systems of type (a) are technically manageable today, and may appear in California as soon as November, 2000, at least on a trial basis. On the other hand, systems of type (b) are vulnerable to Trojan horse attacks for which there are today no good technical solutions that are both effective and convenient enough for voters. Such systems should not be fielded until there is progress on the fundamental problem of managing malicious code." [11] As People for Internet Responsibility noted in a paper[12] released during a wave[13] of attacks on major Internet sites, "Imagine what a concerted denial of service attack might do to an election with Internet/Web-based voting—a technology being pushed on a fast track in many quarters."

Yet another issue of concern is a voter acting under coercion (by an abusive spouse, for example). "Duress alarms" that allow seemingly routine use but signal duress have long been available in combination-driven entry systems and could perhaps be used for this application as well. A number of interesting technical solutions to some Internet voting problems (including tamper-proof smart cards) are proposed in work by Riera.[14]

Finally, should proprietary code be escrowed and examined by election officials (or their experts) as is sometimes now done, or should open source code (perhaps digitally signed to make sure it has not been tampered with) be required? If election software firms can't license open source software, what is a viable business model for them?

Political Issues Raised

A number of political issues have also been raised. What additional training for voters is desirable? Does Internet voting provide (too much of) an advantage for a well-organized fringe group? Does convenience outweigh the possible further erosion of the "civic ritual" of physically casting your vote at your local polling place? "Can technology, through Internet voting or some other process, energize voters and reconnect them to the process?"[15]

David Mason, a Federal Election Commissioner, has pointed out[16] a basic conflict between Internet voting and the current system: **Elections allow chosen intermediaries to be empowered, but the Internet disintermediates.** In a National Review article that commented on the perils of Internet instant democracy, Jonah Goldberg noted that

> In Federalist Number 63, Madison wrote that there are times "when the people, stimulated by some irregular passion . . . may call for measures which they themselves will afterwards be the most ready to lament and condemn. In these critical moments, how salutary will be the interference of some temperate and respectable body of citizens in order . . . to suspend the blow meditated by the people against themselves, until reason, justice, and truth can regain their authority" in public deliberations.
>
> In today's carnival of round-the-clock TV screaming and instant outrage, this concern is even more relevant than it was in Madison's day. Imagine the ill-conceived, MSNBC-inspired legislation that might result from another Oklahoma City bombing. Worse, imagine the incentives for activists and terrorists to stage disasters, if instant democracy were in place.[17]

Writing in the *Guardian*, Hugo Young notes that

> What beckons, in short, is a struggle for the life of representative democracy. An American cynic, observing how absolutely money locks up entry into politics, says that few elected politicians these days are any more qualified than the masses to have an opinion anyway. The special wisdom of public men has gone. A British cynic says that the party whip, and iron executive control, have made it superfluous in MPs anyway: so why not let the people govern by email? [18]

We note that Voter.com, a for-profit site, allows voters to fill out e-questionnaires to search for candidates they agree with.[19] With Internet voting, they could then immediately vote for them, if they trusted the information from that or similar sites.

Privacy and Market Implications

In addition to the usual concern about the privacy of the ballot choice, one can foresee other issues being raised. Suppose a voting system manufacturer offered to impartially run an entire election and bear all the expenses in return for being granted access privileges to market to voters. Should a governmental body even consider such a proposal? Should the voter be able to, or required to, opt in or out before any of this use is made? (Note that in the European Union, laws are much different than in the United States on this issue).

Is it a far stretch to have outsourced elections, such as "County-wide Elections for Prince William County, brought to you by AOL Time-Warner"? How about elections "brought to you" by a smaller vendor, say one of the several already in the business? What if the election service provider is based in a different country than the country of the election?

Additional Readings

There are a number of previous and ongoing studies in addition to the California study mentioned above. The White House has asked the National Science Foundation to look into online voting. The Voting Integrity Project[20] in 1999 raised a number of concerns similar to those in the more recent California report. A recent survey paper[21] surveys the Internet voting landscape in some detail. There are also some earlier studies of the potential and problems of online (not Internet) voting.[22] Finally, Lorrie Cranor's voting page[23] on the World Wide Web and the e-lection mailing list accessible through it point to a wealth of useful information on the topic.

Summary

We have reviewed the promise and potential problems with Internet voting in government-related elections and described some early experiments and reports. We then stepped back and highlighted some political and value-based issues that might remain hidden if not stated explicitly, including potential issues related to the intersection of a market economy and Internet voting. By addressing these issues before they become big problems, we can hopefully achieve the gains promised while solving most of the problems.

References

[1] Raney, Rebecca Fairley, "Voting by the Internet: The Mouse Still Hasn't Roared", New York Times, January 30, 2000, http://www.nytimes.com/library/review/013000internet-voting-review.html

[2] VoteHere.Net to Conduct First Binding Internet Election, press release, VoteHere.net, December 10, 1999, http://www.votehere.net/content/press/991210.asp

[3] Brown, Doug, "The Everywhere Web: Politics: Is Virtual Voting Ready for Real-Time?", Inter@ctive Week Online, January 10, 2000, http://www.zdnet.com/intweek/stories/news/0,4164,2419165-8,00.html

[4] Deborah Phillips in "VIP Files Voting Rights Lawsuit to Block Internet Voting in AZ Democratic Primary", January 21, 2000, http://www.voting-integrity.org/text/2000/rel012100.htm

[5] Carolyn Jefferson-Jenkins, "The Future of Internet Voting", January 20, 2000, Brookings Institution, http://www.brookings.edu/comm/transcripts/20000120.htm

[6] Ann McGeehan, TX Director of Elections at "The Future of Internet Voting", op. cit.

[7] California Internet Voting Initiative, http://www.votation.com/political/civi/civi.htm, accessed February 1, 2000

[8] Richard Wolf, "E-voting glitches must be worked out", USA Today, December 7, 1999, http://www.usatoday.com/life/cyber/tech/ctg837.htm

[9] Davis, Gray and Pataki, George, "Allowing citizens to vote via the Internet", San Diego Union-Tribune, page B-7, January 18, 2000, http://www.signonsandiego.com/news/utarchives/cgi/idoc.cgi?522798+unix++www.uniontrib.com..80+Union-Tribune+Union-Tribune+Library+Library++%28Pataki%29

[10] California Secretary of State, California Internet Voting Task Force Report, http://www.ss.ca.gov/executive/ivote/, January 2000.

[11] David Jefferson, " Internet Voting in Public Elections", Stanford University Computer Systems Laboratory Colloquium, January 5, 2000, http://www.stanford.edu/class/ee380/, viewed February 1, 2000

[12] People for Internet Responsibility, Statement on Recent Internet Denial of Service Attacks,

February 9, 2000, http://www.pfir.org/statements/02.09.00

[13] Matt Richtel and Joel Brinkley, "Spread of Attacks on Web Sites is Slowing Traffic on the Internet", *New York Times*, February 10, 2000, http://www.nytimes.org/library/tech/yr/mo/biztech/articles/10web.html

[14] A. Riera. *Design of implementable solutions for large scale electronic voting schemes*. PhD thesis, Universitat Autònoma de Barcelona, Departament d'Informàtica, 1999. (Project TEL97-0663), http://www.ccd.uab.es/~andreu/indexenglish.shtml

[15] Davis and Pataki, op cit.

[16] "The Future of Internet Voting", op. cit.

[17] Jonah Goldberg, Vote.con: The perils of "cyber-democracy", National Review Online, December 20, 1999, http://www.nationalreview.com/20dec99/goldberg122099.html

[18] Hugo Young, The internet will take over politics in good or bad ways, Guardian Unlimited, January 6, 2000, http://www.newsunlimited.co.uk/Print/0,3858,3947574,00.html

[19] Elizabeth Wasserman, "Profiting from Politics", *The Industry Standard*, Nov. 22-29, 1999, http://www.thestandard.com/article/display/0,1151,7606,00.html

[20] Deborah Phillips, "Are We Ready for Internet Voting?", http://www.voting-integrity.org/projects/votingtechnology/internetvoting/ivp_title.htm

[21] Derek Dictson and Dan Ray, "The Modern Democratic Revolution: An Objective Survey of Internet-based Elections", January 18, 2000, http://www.securepoll.com/VotingPaper.htm,

[22] Roy G. Saltman, "Assuring Accuracy, Integrity and Security in National Elections : The Role of the U.S. Congress", Proceedings of the 3rd Conference on Computers, Freedom, and Privacy, 1993, http://www.cpsr.org/conferences/cfp93/saltman.html

[23] http://www.research.att.com/~lorrie/voting/