BUSINESS 2.0

FUTURE BOY

Internet Voting: What Are We Waiting For?

Electronic voting is just the first step to truly democratizing the election process.

By Erick Schonfeld, October 29, 2004

On Election Day, as many as 30 percent of voters will cast their ballots on electronic voting machines. And what a storm of controversy that has created over the accuracy and security of those ballots. One of the biggest concerns is that if a recount is ordered, there will be no paper trail for many of these machines. Still, despite their problems, such machines represent the first step toward a worthy goal: not just electronic voting, but Internet voting.

None of the electronic voting machines in this year's election will be connected to the Internet because of fears of hacking, fraud, and compromised security. But if I can bank online, trade stocks online, and shop online with confidence, why can't I vote online? Internet voting holds out the possibility of increasing voter turnout, reducing human errors, and making voting easier and more convenient, just as ATMs made banking so much simpler.

Online banking has enhanced our life even more. Why couldn't balloting follow the same technological path? "Voting is probably one of the last institutions that does not resonate with our lifestyle," argues Jim Adler, founder and CEO of electronic voting technology startup VoteHere. "Look at this election," he says. "People have a real will to vote, but are bumping up against a lot of friction, whether that is due to bureaucratic regulations or Election Day issues like parking and polling access." In Britain, his company has been involved in successful experiments with Internet voting, as well as in voting with regular touch-tone phones, with text messages on cell phones, and with interactive TV.

Like banking, an election is ideally suited for computers because it is essentially an accounting procedure. And computers are better at counting than humans. "Paper audits are just completely useless," says Ted Selker, co-director of the CalTech-MIT/Voting Technology Project. According to him, in the last presidential election 2 percent of the ballots were lost because of human error or outright fraud. "Whenever you have paper," he says, "people get their hands on it. Last election, they found ballots floating in the San Francisco Bay." (Actually, only the ballot box lids were found.)

Electronic voting on touchscreen machines has its own problems, of course. But by fixing some of them, many of the hurdles preventing Internet voting will be surmounted as well. These include making sure voters are who they say they are before allowing them to vote (authentication), making sure everyone who wants to can use the system (access), making sure voters have a way of checking to see that their votes are counted (verification), and making sure there is an audit trail that anyone can follow (transparency). Luckily, some smart computer scientists like David Chaum, Ronald Rivest, and Selker are working to solve these problems.

The first issue is authentication, ensuring that each person gets one vote (and only one vote). Voters should be authenticated more than once using two or more ways: passwords, questions only they know the answers to, digital signatures, or identity tokens with flashing numbers that change every minute. If there are at least two different authentication methods, a case can be built that the people voting are who they say they are. But what about coercion? Wouldn't it be easy for a boss, say, to force all his workers to vote a certain way, or for a party operative to buy votes? Safeguards could be put in place to thwart these scenarios, such as allowing people to vote as many times as they want but make only their last vote count, or letting them enter a distress code instead of their password, or setting up secure polling places that trump any other votes people might have cast online.

As for access, 70 percent of the U.S. population is already online, as are most schools and libraries. Nevertheless, those who still prefer to go to polling places and yank creaky old levers or punch chads should be free to do so. Hopefully those systems will be updated, though, so that the voting experience is the same whether you do it from home or at a voting kiosk in a polling place.

One of the trickiest issues is verifying that no one has tampered with electronic ballots. "What I discovered," Selker says, "is every time elections have been improved it is because people have been watching each other's work. Why don't we have computers do that too?" He's come up with an electronic voting system that would have multiple pieces of software handle each stage of the voting process and demonstrate to one another that they always get the same answers for each vote cast.

But what people really want -- and what would ease a lot of fears -- is the ability to get a paper record of their vote, just like they get a receipt at an ATM. "Any electronic transaction," Adler points out, "whether at the gas pump or tracking a FedEx, provides you with some verification that your transaction was captured correctly, and that can then always be verified against some statement of account." Voting should be the same. Except with voting, since the sanctity of the secret ballot must be protected (and you don't want people cashing in those receipts for voting a certain way), any paper record cannot explicitly say whom you voted for.

Adler's company, VoteHere, fulfills the secrecy requirement by printing the equivalent of a confirmation number on your record, so that you can later check online to make sure your ballot was counted. You can also pick a PIN for any individual candidate selection you want to verify. Adler explains, "The machine can't cheat you without cheating that receipt." (Selker thinks we should forget about paper records altogether and just convert each vote to audio as a backup. It would be recorded on a tape that voters could review before leaving the polling booth. If part of the tape were to be erased, that could be evidence that the vote was tampered with.)

Finally, there's got to be a way to systematically audit election results. Adler publishes all the algorithms and source code for his software so that anyone can go back and check the results. "The security does not rely on the software," he says. "It relies on the data that gets published. We want there to be enough transparency so that if anyone does cheat or make a mistake, you can see it." That is a sound principle, and a very democratic one. Why should we rely on Republican or Democratic functionaries to certify our elections? (They are all too often the ones we need to worry about the most.) As a necessity, Internet voting would force our elections to become even more open to scrutiny than they are today. And that would be good for democracy. ✦

Erick Schonfeld eschonfeld@business2.com is an editor-at-large for Business 2.0.

Find this article at http://www.business2.com/b2/web/articles/0,17863,735959,00.html.

Try a Free Issue of Business 2.0: Call (800) 317-9704

Recent Future Boy Articles

- Amazon, eBay, and Google Turn Themselves Inside Out
- Political Campaigns Are Missing the Boat on Paid Search
- Smart Dust Comes Out of the Labs
- Technology Equals Democracy
- Nanotech Needs