

Online Democracy

Why the Era of E-Voting Will Have to Wait

Back in the 1990s, when every day was a sunny day and the future had a dot-com after its name, it seemed certain that by 2004 people would be voting online. The idea was simple: rather than trudging out to the polling place, standing in line, and pulling a lever, citizens could log on from the comfort of their home, prove their identity, click on their choice, and play their part in American democracy, all without putting their shoes on.

Well, the future is here, and our shoes are still on. As a result of the controversy surrounding the 2000 presidential election, Congress passed the Help America

Vote Act, which made available nearly \$4 billion for improving the nation's voting systems, and prompted many states to consider the future of computerized and Internet voting. Some limited trials of online voting have been undertaken, most notably in Arizona's Democratic primary in 2000 and in the Michigan primary this year, but concerns about safety have kept experiments to a minimum. In 2001, the Internet Policy Institute carried out a major review of the options for Internet voting, financed by the National Science Foundation. The study concluded, in no uncertain terms, that "remote Internet

voting systems pose significant risk to the integrity of the voting process and should not be fielded for use in public elections until substantial technical and social science issues are addressed.”

The technical issues have especially to do with security. If an Internet voting system were hacked, the hackers would have the power to alter election results, or at the very least to place results in serious doubt and dispute. Interested parties and opposing candidates might try to exploit the weak security and pick the winner. And for some malicious hackers—not to mention terrorists—disrupting the fundamental instrument of American democracy would be a dream.

Another worry relates to fairness, and the possibility of restricting voting to those with computer skills and Internet access. (Imagine a polling place that only allowed those who could afford a computer to vote.) It is also far from obvious whether accommodating people who are too lazy to leave their computer once every few years to go vote would benefit American democracy.

But daunting as the problems remain, the appeal of Internet voting is great, particularly to voters who live far from polling places and who could never be accused of laziness—like American soldiers abroad. The Defense Department, through its Federal Voting Assistance program, has been developing a system called the Secure Electronic Registration and Voting Experiment, or SERVE. The system was designed to be used on a trial basis by some states during the 2004 primary election season, and then to be used in the general election by Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington, allowing residents of those states who were sta-

tioned abroad to vote online from any Internet-enabled computer. Eventually, it was thought that the program could be expanded to provide voting services to all eligible overseas citizens, including both civilians and military personnel and their dependents—a population that exceeds five million Americans.

But as the system was nearing its first phase of use, a panel of government-commissioned experts released a report in mid-January raising serious questions about security. The panel concluded that SERVE has “fundamental security problems that leave it vulnerable to a variety of well-known cyberattacks, any one of which could be catastrophic.” Such attacks, they worried, “could have a devastating effect on public confidence in elections.”

A new method of voting, the panel argued, should not be allowed to introduce serious new risks that were never otherwise present. The SERVE system exposes the election process to the dangers of viruses, worms, hackers, and intruders, and gives up too much security for the sake of convenience. The problem, according to the report, was not the fault of the Pentagon, or of Accenture, the company that built the SERVE system and software. Indeed, the panel remained sanguine about the future potential of such technology in any form, writing that “there really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough. The SERVE project is thus too far ahead of its time, and should wait until there is a much improved security infrastructure to build upon.”

Officials at the Pentagon were swayed by the panel’s argument: On January 30, 2004, Deputy Defense Secretary Paul Wolfowitz ordered that all efforts to move

ahead with the SERVE project be halted, at least until “it can be shown that the integrity of the election results can be assured.”

This cautionary course reflects a principle articulated in the first serious examination of online voting, the 2000 report of the California Internet Voting Task Force, a working group of election and computer specialists organized by California’s Secretary of State. The task force recommended an “evolutionary” rather than “revolutionary” strategy for the implementation of Internet voting: Before we even consider the possibility of remote voting over the Internet, computerized voting systems should first be used in traditional polling places, where they can be closely scrutinized and shown to be completely free of security vulnerabilities, technical and otherwise.

But building an electronic voting machine with chink-free armor has proven immensely difficult. The voting machines manufactured by Electronic Systems & Software are presently under investigation for losing ballots cast in elections in North Carolina and Florida. And last year, two other leading electronic voting companies, Diebold and Sequoia, were left red-faced when it was discovered that the proprietary code they developed for their voting

machines had been leaked over the Internet. The leaks raised concerns that a Trojan horse—code designed and surreptitiously implanted by hackers—could alter the tabulation process in voting machines, thereby affecting election results. As a result, proponents of Internet voting have argued that open source software, rather than the proprietary software of Diebold and Sequoia, is the only way to allow public oversight of elections and ensure that voting machines are tabulating and registering votes the way that voters had intended.

But even open source software isn’t sufficient, says Rebecca Mercuri, an Internet voting analyst at Harvard’s Kennedy School of Government. “To have a fair, democratic election, there has to be a visible, transparent way of performing recounts and confirming that ballots have been correctly cast.” Electronic voting machines, let alone personal home computers, presently offer no way of performing an independent audit of election results to insure that votes were recorded in the way voters had originally intended.

The concept of electronic and online voting still makes some sense in principle, but as long as practical problems of this scope remain, it may truly be “too far ahead of its time.”