PLAN FULL OF FLAWS

Internet voting short on security

By Deborah M. Phillips
and Hans A. von Spakovsky

In just weeks, Arizona Democrats will allow remote voting by computer in their upcoming presidential primary. A number of states, including California, are studying the implementation of Internet voting.

But are we really ready for Internet voting? Voting is our most basic and important right as citizens. Any method of voting must guarantee ballot secrecy, ballot sanctity and equal access to the ballot box. Yet states and political parties are proceeding before anyone has proven that these three guarantees can be met with Internet voting.

Ballot secrecy and ballot sanctity require a secure voting system that verifies the identity of the voter, allows a vote to be cast anonymously, and does not allow the vote to be changed after it has been cast. It is not yet clear that Internet voting can consistently meet any of these requirements.

The Internet was never constructed to be secure. Security lapses, such as attacks on government Web sites, computer virus propagation and system shutdowns, are common. The open architecture of the Internet and the required accessibility of government computers that would be used by voters to cast their ballots make this type of voting vulnerable to outside manipulation and fraud.

Statewide computers that are receiving and counting votes in a presidential election and are accessible worldwide through the Internet could be irresistible targets.

■

In addition to hackers, other dangers are appearing on the technology horizon. The Pentagon recently revealed that the Chinese government has set up a special Internet and computer warfare unit.

Although it might now seem difficult for a foreign government to commit voter fraud in individual precincts, statewide computers that are receiving and counting votes in a presidential election and are accessible worldwide through the Internet could be irresistible targets.

Arizona is moving ahead with on-line voting even though none of the Internet voting equipment being marketed has been certified by the Federal Election Commission or any state election officials. The FEC has not yet even prepared any performance standards for this type of equipment. If fraud were to occur, it is not clear that election officials would even be able to detect it.

Verification of a voter's identity is obviously a key element of our election process. Therefore, even if a perfectly secure Internet voting system could be designed, current problems with our voter registration processes have to be corrected before any such system is used. There is really nothing to prevent someone from registering under a false name numerous times, and examples of false registration records have been found all over the country.

There has been much discussion lately about a digital divide. Current studies show that those most likely to access the Internet are white, college-educated males under 35, with above-average incomes. Making it easier for that segment of the population to vote with their home computers may add a bias to the process that will affect election outcomes. Internet voting could wind up being the New Millennium version of the literacy test.

Finally, we should not make the mistake of implementing Internet voting because we think it will reverse the 30-year decline in voter turnout. The decline in turnout is not a problem caused by the mechanics of voting.

The integrity and security of free and fair elections are too important to our democracy to be sacrificed on the altar of new technology without long and careful review. The move toward Internet voting can be likened to a loaded semi barreling down the highway in heavy fog with no lights and no brakes.

Deborah M. Phillips is president of the Voting Integrity Project, which recently released the first study on Internet voting. Hans von Spakovsky is a member of the National Advisory Board of the Voting Integrity Project and a member of the Fulton County Board of Registration and Elections.