transparency compared to our traditional machine- and paper-based electoral processes. Internet voting can be implemented only with absolute commitment to maximum inclusiveness and accessibility for all voters.

51

"Gauging the Risks of Internet Elections"

DEBORAH M. PHILLIPS AND HANS A. VON SPAKOVSKY

The idea of voting via the Internet has fired the imaginations of many millions of political professionals, office holders, and voters in the U.S., as well as around the world. Several state legislatures, including those in Georgia, Illinois, and Ohio, are considering Internet voting bills, and California last year studied the technology. As voter turnout has continued to decline across the U.S. Internet voting initially presents itself as a benign, even benevolent, new platform for election administration, promising to reach voters not currently engaged in the process. However, Internet voting is fraught with risks to the integrity and security of elections.

Since all American rights and freedoms derive from the exercise of the voting franchise, it is a puzzle why voter turnout continues to decline. Major reforms, including no-fault absentee balloting and early voting, enacted in the hopes of increasing turnout by making voting more convenient, have failed to achieve their goals and may even be contributing to the decline. Before employing yet another strategy to address the problem, we must assess the potential risks and benefits of using the Internet as a voting mechanism. Here, we review the important public policy questions, as well as the technology challenges, using as our gauge the three critical tests—security, privacy, and equity—for considering whether an election is free and fair.

Free and Fair?

California's Internet Voting Task Force concluded in 2000 that the "technological threats to the security, integrity, and secrecy of Internet ballots are significant." The Task Force, which included technology experts, political scientists, civic leaders, and election vendors, reported how an Internet voting system could be undermined by virus attacks and fraud, concluding that, today, "it would not be legally, practically, or fiscally feasible to develop a comprehensive remote Internet voting system." It

also recommended that the first use of Internet technology in elections be confined to public polling places under the watchful eyes of election officials.

The Internet involves an open architecture that never contemplated the security issues now gripping the Web. The Arpanet, the Internet's predecessor network, was created to facilitate global information exchanges between government and academic users. E-commerce and other transaction applications have been added to that framework, and security has been retrofitted. A passionate debate is now being waged by these various user groups over how much privacy and freedom has to be sacrificed to facilitate new users without destroying the free exchange of ideas, access, and traffic that characterize the Web.

Internet security is usually just one step ahead of the next creative assault; public resources to protect users are woefully deficient. Attacks on commercial and government Web sites, computer virus propagation, shutdowns caused by event-driven traffic and deliberate denial-of-service attacks are commonplace on the Internet. The public is not generally aware that, even on "secure" sites, they may be vulnerable to password theft, credit card theft, and the wholesale snooping and misuse of private information. Internet elections would be vulnerable to the same types of activity. For example, a report released in 2000 by Carnegie Mellon University warned "[t]here is essentially nothing a site can do with currently available technology to prevent becoming a victim of . . . a coordinated network flood". Could future cyber-voters be denied their franchise in such scenarios?

Although breaks are possible at virtually every link in the election chain in the Internet-based voting systems being contemplated, the Federal Election Commission is not even close to promulgating technology or administration standards for these systems. Even if a truly secure Internet system were created, it would still rely on registration records that are increasingly corrupted with "dead wood" and fraudulent names. By removing elections from independent public scrutiny, Internet voting may offer a cloak for fraud.

Remote Internet voting assumes a secure infrastructure of voter terminals that does not exist. The average computer user is unschooled in defensive tactics, as evidenced by recent virus and worm attacks. A Trojan Horse virus could be lodged on a computer and manipulate a voter's ballot without detection. Although individual users are the most vulnerable, even networked users guided by professional administrators might inadvertently import such devices through management software. Even systems controlled by election officials might be vulnerable.

When the U.S. military staged a pilot project in the November 2000 U.S. general election, allowing 250 selected military personnel to vote overseas via the Internet, it did so only on certified "virus-free" machines at military bases.

Voters casting ballots on computer terminals or whose paper ballots are scanned electronically and tabulated often question the potential for unseen manipulation. Completely removing voting from independent observers and putting it in cyberspace may stretch the public trust to the breaking point. An essential element of secure and fair elections is the ability of independent observers to monitor all aspects of the election process, from voting in polling places to ballot counting in vote tabulation centers.

The resistance shown by Internet vendors to any independent testing of their systems is disturbing. Because Internet elections are a potentially lucrative and competitive emerging market, vendors are understandably wary of opening their proprietary systems to public scrutiny and competitor theft. However, an independent framework for scrutiny of these systems by knowledgeable experts and public observers is essential.

The U.S. has an unfortunate history of voter fraud. Until recently, most incidents were limited to smaller elections at the local level. Public scrutiny in polling places made it difficult to successfully conduct organized vote theft on a wide scale, though that is changing.

Mail-in absentee balloting offered the first indication that removing the process from the polling site only makes the vote thief's job easier. As more and more states have relaxed rules for casting mail-in ballots, absentee-ballot fraud has increased. A 1998 report by the Florida Department of Law Enforcement (after the 1997 Miami mayor's race was thrown out due to massive absentee ballot fraud) concluded that absentee ballots have become "the tool of choice for those who are engaging in election fraud." But such fraud is labor-intensive.

Internet voting would upgrade the vote thief's technology while simultaneously moving it farther from public scrutiny. Moreover, in addition to the local vote thief, Internet elections may attract a new kind of attention—foreign intelligence agencies and terrorists who might view U.S. elections as tempting targets for manipulation or interference.

All of these vulnerabilities demand that any Internet election must have acceptable, standardized systems for archiving votes, allowing recounts and audits as to content, results, and process at a level sufficient to guarantee the security of the system, as well as the public's confidence in election outcomes.

Secret Ballot

The secret ballot originated in Australia and is often referred to in history texts as the "Australian ballot." It was instituted in the U.S. in Massachusetts in 1888 and is important for preventing coercion, as well as vote tampering. Remote Internet voting—at home, work, the local library—makes virtual voting vulnerable to violations of secrecy. Spouses or parents who would be privy to personal identifiers needed to "secure" on-

line voting could coerce or simply vote in place of family members. Voters using their networked office computers could have their ballots read or changed by network system administrators. Employees would have to trust that administrators had set up privacy buffers to prevent such snooping and alteration.

Remote Internet voting in unmonitored settings lacking election officials or independent election observers might encourage electioneering or organized voter coercion by employers, churches, union bosses, nursing home administrators, and others. Laptops now prevalent in campaign organizations could be used to "turn out the vote" in favorable precincts removed from the scrutiny of election officials or poll watchers, a logical extension of the kind of fraudulent activity currently conducted via absentee mail-in balloting today.

Equity

The U.S. civil rights movements of the past century have centered on achieving equity of access to the ballot box. Once the vote was secured for minorities, creative devices, such as "literacy" tests, were often used to systematically prevent or suppress the exercise of the franchise. In fact, though some may believe such tactics are a thing of the past, states with a history of election discrimination are still under the watchful eyes of the U.S. Justice Department and must "pre-clear" every change in election administration before it occurs to ensure it will not interfere with the rights of minority voters. There is a good case to be made that, given inequities of access, remote Internet voting represents a new-millennium version of the literacy test.

One of the most comprehensive studies on this issue, *Falling Through the Net: Defining the Digital Divide,* was published July 1999 by the National Telecommunications and Information Administration of the U.S. Department of Commerce (see www.ntia.doc.gov). It reported that whites are more likely to have Internet access at home than most racial and ethnic minorities from any location, including home, work, school, and library. 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. All told, African-American and Hispanic households are only 40% as likely as white households to have home Internet access. The Digital Divide is growing, because, although minorities are slowly gaining access, whites are accelerating their access. Simple economics are not the engine driving this disparity. Among individuals with incomes of $20,000 or less, whites are five times more likely to have Internet access than minorities.

Even if special care is taken to create "cyber villages" in publicly accessible locations, remote Internet voting would still be less likely among minority voters. By making voting more convenient for voters with

ready access—predominantly white—a bias is set up that boosts the potential turnout for connected voters while simultaneously diluting the power of individual minority voters' ballots. If someone suggested adding polling locations to majority white precincts, that person would be run out of town. Yet that is the practical effect of conducting elections that give a significant access advantage to certain voters.

The implications are profound. Remote Internet voting could be used to manipulate election outcomes by structuring access to favor those who are the most Internet-connected. For example, in a statewide referendum election on permitting a toxic waste dump to be located in a predominantly minority jurisdiction, Internet voting could be employed to flood the election with favorable votes from white voters outside the jurisdiction with greater access to the Internet to the disadvantage of those most likely to be affected—minority voters in the jurisdiction with much less access to the Internet.

Equity of access is addressed by removing remote Internet voting from the election equation. By confining Internet voting to polling places, the immediate result is parity, while gaining time to address the complex issues of how to bridge the divide. Anthony Wilhelm, program director of the Communications Policy Program at the Benton Foundation in Washington, DC, concluded recently that "[o]nce communities are wired and the Internet becomes second nature, Internet voting, done responsibly and with proper securing safeguards, will surely take off. The day will come when Internet voting is available on terms acceptable to all. That day has not yet come."

The 2000 Arizona Primary

The March 2000 Democratic presidential primary in Arizona was the first binding public election in the U.S. to use Internet voting technology. Held outside the state-conducted (and state-funded) primary, the Arizona Democratic Party had to deal with generating interest in an off-cycle election while keeping costs down. The Party recognized that conducting the "first-ever" binding Internet election would not only generate enormous media interest, hopefully resulting in greater turnout, but enable the Party to keep down costs by reducing the number of public polling places needed. The original announced plan envisioned four days of around-the-clock Internet voting with only 12 hours of public balloting limited to fewer than 100 polling places—in a state that normally opens more than 2,000 neighborhood polling places for a statewide election.

Although Arizona is one of the states still required to seek "pre-clearance" of any election change, the Arizona Democratic Party took the position that it was not required to seek and obtain pre-clearance for

its Internet voting plan. The Voting Integrity Project, a nonpartisan voting-rights organization in Arlington, VA, and its minority voter co-plaintiffs, concerned that an injustice was about to be perpetrated, brought a federal voting rights lawsuit in Arizona district court alleging that Justice Department pre-clearance was indeed required and the way the election was structured would almost certainly result in injury to minority voters (see www.votingintegrity.org).

The case forced the Party to file for pre-clearance, expand the number of public polling places, and add a mail-in ballot component to the election. In granting pre-clearance, the Justice Department expressed its extreme concern for the potential for discrimination in the election, as did the federal judge hearing the injunction motion. Stating he suspected "there is a digital divide that may well result in racial discrimination . . . ," he nevertheless permitted the election to proceed, warning he would not hesitate to set aside the results if warranted. A trial is set for April 2001. The judgment resulting from this trial will set a precedent for other states contemplating Internet elections.

Preliminary results from the Arizona primary showed that large urban counties with predominantly white voter populations vote via the Internet in much greater numbers than their counterparts in rural counties with large populations of minority voters. The Voting Integrity Project is still gathering data to support its contention that the election violated the Voting Rights Act of 1965.

All 849,000 registered Democrats in Arizona were mailed a PIN number that could be used, in combination with other personal information readily obtainable on the Internet, to cast ballots. It is not inconceivable that such lax procedures could have resulted in the sale of votes among the 39,942 ultimately cast over the Internet (another 46,028 were cast through traditional means). Other problems were encountered by Macintosh users and voters with certain older Internet browsers unable to access the system. However, we do not know how many voters were prevented from voting due to these technical glitches; the vendor did not keep track of these attempts. Other voters who lost or did not receive their PIN numbers were unable to get through via telephone to the Democratic Party to obtain their numbers; computer users calling in with browser problems flooded their phone lines. Finally, the system apparently was not compliant with Americans with Disabilities Act specifications for the blind; blind voters attempting to vote via the Internet were met with silence whenever there should have been auditory prompts.

Another potential weakness received little attention in the media. The primary relied heavily on voter access from offices and public libraries —networked computer environments that could have been compromised easily as to security and privacy. Still unknown is the extent of efforts made to protect their ballots.

Why Bother?

The Voting Integrity Project asked whether any precinct in the entire U.S. was even ready for Internet voting in a 1999 article (see www.votingintegrity.org). A number of public polls reflect wariness about Internet elections but also indicate openness to the idea at some point in the future. However, a growing number of critics are asking a more fundamental question: Why do it at all?

Convenience represents one of the best arguments for Internet voting. A public that initially resists and then accepts automated versions of various personal transactions, including banking, supermarket checkouts, even medical procedures, is likely to accept Internet voting eventually. But we should also be asking whether such acceptance would yield desirable public benefits. Unlike personal transactions, casting a vote is a public act that may best be limited to public environments, unless there are compelling reasons to change.

One such compelling reason might be if Internet voting offered any real hope of addressing the decline of voter turnout. The U.S. form of government depends on an active and engaged citizenry, yet today, diminishing numbers of Americans routinely cast ballots. The 49% turnout in the presidential election of 1996 was the lowest in an American presidential election since Calvin Coolidge was elected in 1924 and the second lowest since 1824; the 36% turnout in the 1998 election was the lowest in congressional elections since 1942.

Well-intentioned reforms enacted to address this 30-year decline in voter turnout may actually have contributed to further declines, particularly among the most-likely voters. The National Voter Registration Act (also known as "Motor Voter") of 1993 eliminated almost all registration requirements and mandated simple mail-in registration. It has resulted in a huge increase in registrations—not in voters. "Early voting," another reform now employed to some degree in a number of states, permits casting a ballot in person prior to an election day but generally has not increased turnout.

Absentee balloting is no longer limited to those unable to cast their votes in person for physical or employment reasons. In a growing number of states, it is available without cause; in Oregon, it has become the default voting method. But in its first statewide primary and in the 2000 general election, Oregon's vote-by-mail process was accompanied by a host of problems, including extremely delayed vote counts.

The Voting Integrity Project finds the main reason voters do not vote is they do not believe their votes matter for a variety of reasons. That is why convenience alone does not motivate voters to get to the polls. Novelty, on the other hand, which can excite turnout, typically provides only a temporary turnout increase.

Still unclear is whether Internet voting contributed to increased voter

turnout in Arizona in the 2000 primary, despite the claims of the vendor, since the most recent comparable election was not at all equivalent. The previous Democratic presidential primary in 1996 had only one incumbent candidate, whereas the one in 2000 started out competitive. Still, only 10% of the state's registered Democrats turned out to vote. By comparison, 35% of registered Republicans turned out in their primary using traditional voting sites. Quite clear, however, is that there was substantial use of the Internet voting available; it remains to be decided in court whether it provided a discriminatory margin of votes.

* * *

Framework for Progress

Internet elections may be inevitable, assuming the Digital Divide is overcome through uniform Internet access. But to prevent premature or injurious use, we offer the following framework and its guidelines for progress.

Assess the Desired Benefits

Assess the desired benefits of election reform, including Internet elections, before implementation. Is there a reasonable expectation the reform will result in the desired outcome? And most important, what are the potential unintended consequences?

Let the Sun Shine In

Know which vendors the state does business with, limiting their ability to illegally or inappropriately influence contracting. Also limit accessibility to vendors owned and controlled by domestic organizations. Foreign governments often use commercial interests to achieve political ends in the U.S.

Use Citizen Poll Watchers

State statutes provide for citizen poll watchers, usually under the auspices of political parties or candidates; whose only role is the independent monitoring of election integrity. This function is essential to maintaining public confidence in election outcomes. If election officials embrace this role, it can also be used to build public engagement in the political process and increase voter turnout. The Voting Integrity Project has constructed an initial framework for citizen poll watchers in cyberspace. It would require setting up a computer monitor allowing observers to see selected information on voters as they log into the official

election Web site to cast their ballots. This special access would allow the observers to compare the names and addresses of the voters with the official registered voter list to make sure only registered voters are actually voting. Other information about the voting system could also be displayed to help observers monitor the tests election officials usually conduct of their vote-tabulation software prior to the start of the processing and counting of ballots. This concept of trustworthy public scrutiny would require extensive development and testing to determine whether it provides a comprehensive method for citizens to monitor such elections.

Set Standards

Set standards for any new voting system—especially Internet voting—before elections are conducted using it. These standards must ensure equity, security, and privacy and are reflected in the Voting Integrity Project's draft model legislation, which suggests thresholds for implementing Internet voting.

Conclusion

The U.S. form of government depends on an engaged and active citizenry. Free and fair elections secure their rights and freedoms. Internet voting may solve many of the problems they face in elections today but should be allowed to proceed only after careful and deliberate public debate as to whether it will produce outcomes that are indeed desirable. Premature implementation, without sufficient testing and constraints, risks inequity, fraud, and the fundamental loss of freedom.

52

"Voting Alone: The Case Against Virtual Ballot Boxes"

RICK VALELLY

It's not often that a special school district vote has the potential to alter the course of American politics. But last April, when residents of the Puget Sound city of Shelton, Washington, cast their votes on questions such as whether the Pioneer school district should have "full-day kin-