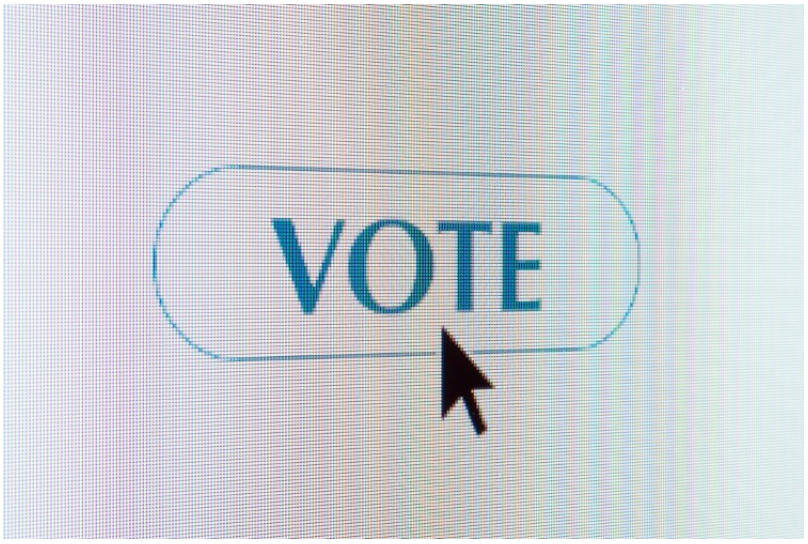
Written by **Kurt Hyde** on October 9, 2000

Voting on the Web

On March 11 of this year, electoral history was made in the state or Arizona. There, for four days ending on the 11th, the state's Democratic primary became the first legally binding online vote in the nation's history. The idea of using the internet as a voting medium is not new; *USA Today* reported last December that the Clinton administration had instructed the National Science Foundation to conduct a one-year feasibility study of online voting. But the Arizona Democratic Party thrust us into the brave new world of virtual balloting before we were aware.



stockcam/iStock/Getty Images Plus

Arizona's online voting, which was carried out under contract by the private firm election.com, provoked a strong response from proponents of equal and universal electoral access. Professor Michael Cornfield of George Washington University argued that "it just wasn't fair to give people who had Web knowledge and Web access four more days to vote than people who didn't." Deborah Phillips, president of the Voter Integrity Project, commented that "the window of voting opportunity for non-Internet-connected voters was very narrow. The window for Internet users was very wide.... It is not rocket science to conclude that the Arizona model would result in a disproportionate number of white voters being able to vole. We are looking at a drowning out or the minority vote." The Voter Integrity Project subsequently filed a lawsuit questioning the legitimacy of the election. Yet beyond such peripheral concerns for the rights of allegedly put-upon minorities, the prospect of Internet voting raises some very serious questions about the potential for electoral abuse.

Vote fraud, to be sure, has always had a hand in American politics. In the 1948 Texas Democratic Senate primary, for example, the evidence suggests that Lyndon Johnson and his cronies manufactured enough fictitious votes to steal a close runoff election from former Governor Coke R. Stevenson. John F. Kennedy may have benefited from vote fraud in Illinois and Texas during the 1960 presidential race against Richard Nixon. In a more recent example, Democratic challenger Loretta Sanchez' upset win over Republican House incumbent Robert Dornan in 1996 was clouded by credible allegations that enough non-citizens and other ineligible voters cast ballots in that election to cast into doubt the outcome. Overall, though, our elections are both fair and open to public scrutiny, in stark contrast to most of the rest of the world. Internet voting, however, introduces frightening new possibilities for abuse and fraud on a far greater scale than before. The internet is so inherently insecure — and is likely to remain so for the foreseeable future — that it is a veritable open invitation for electronic tampering. We have all seen in recent months how vulnerable the internet is to computer viruses and denial-of-service attacks. There is absolutely no reason that internet votes could not easily be disrupted in similar fashion, either by viruses programmed to alter the results of balloting or by denial-of-service attacks that shut clown the system altogether. In addition, any individual or group with inside access to passwords or electoral computer systems could conceivably tamper with election results.

Electronically stuffing the ballot box is one of the biggest potential security flaws in any computerized

vote-counting system, internet-based or otherwise. A computer could be programmed, for example, to check vote totals after the polls close, and then cast the required extra ballots, checking off the names of voters who didn't vote. Or a virus might be implanted with the ability to change voters' ballot choices after they have been submitted. With these and a host of other potential strategics for electronic ballot-tampering, the greatest threat is not that they are likely to occur, but that they will be difficult to detect and almost impossible to trace. Electronic transactions leave no paper trail, are not subject to manual recount, and may originate anywhere.

One proposed solution to internet voting security issues is the use of biometric identifiers such as electronic fingerprinting and retinal scans for online voters. Deborah Phillips and David Jefferson of the Voting Integrity Project, in their paper "Is Internet Voting Safe?" observed wryly: "Aside from issues or cost and infrastructure, biometrics have not been embraced by the public because of … privacy concerns."

For those of us alarmed at the prospect of national ID cards complete with biometric identifiers, the possibility of such a system of identification, ostensibly for secure internet balloting, ought to sound alarm bells. Moreover, if electronic biometric identifiers ever became universally adopted for security purposes and commercial transactions, they would likely be just as susceptible to theft and fraudulent use as are today's social-security and credit-card numbers.

Denial-of-service attacks, such as those that crippled internet giants such as Yahoo and eBay earlier this year, are another realistic threat to online votes. On April 6, the *Wall Street Journal* reported what may have been the first politically motivated e-attack to receive attention in the news media. Juergen Ruettgers, a conservative Christian Democrat candidate in Germany, had his email shut down by a deliberate flood of thousands of messages sent by the Greens, a rival party.

In an interview with *The New American*, Joseph Mohen, CEO or election.com, admitted that the Arizona Democratic primary was e-attacked. There were two kinds of attacks, denial-of-service and password--guessing, all of which were successfully thwarted. Nevertheless, the fact that this first-ever, true internet election was subject to such sabotage attempts shows the profound weaknesses of internet voting. Attacks on future internet elections may be prosecuted more successfully.

Nor can we exclude the potential for foreign enemies to disrupt online voting in the United States in what would amount to cyber-terrorism and even cyber-warfare. We can only speculate how many hostile foreign powers might have the capability to break into election computers and alter voting results.

Yet despite such obvious risks, there is now a significant push underway to bring about generalized internet voting as quickly as possible. Besides the Arizona Democratic primary, several other states have experimented with internet voting this election season, though no other state has conducted a legally binding vote. The Alaska straw poll on January 24, which allowed participants to vote online, did not attract much attention at the time, and for good reason: Out of 4,000 votes, only 35 were cast via the internet. Iowa plans experimentally to allow voters to cast their ballots by Internet, but only after they have first voted in the traditional manner. Washington state has conducted a few non-binding local internet elections, involving at most a few thousand votes. Yet Washington's Secretary of State John Pearson recently expressed skepticism that internet voting is feasible on a larger scale: "We know we can handle 3,000 voters…. Can we handle 300,000 or 3 million?" A number of other slates, such as California, have created task forces to actively study the advantages and disadvantages of internet voting.

Overall, the commonly held assumption, at least in political circles, is that internet voting is inevitable, and that, in the not-too-distant future, John Q. Public will be able to vote for congressmen and presidents with the same point-and-click convenience he enjoys when shopping on Amazon.com. As New Mexico Secretary of State Rebecca Vigil-Giron predicted confidently, “The question isn’t whether we’ll have Internet voting, but when.”

But the interest in internet voting is based more on the inherent lure of technological novelty than on sound political wisdom. The fact that internet voting is already possible doesn’t make it advisable, given its vulnerability to security breaches — unless the goal is to deliberately weaken the American electoral process. That current security problems may eventually be reduced does not mean that an electronic medium, where information is always evanescent, can ever be as reliably monitored as old-fashioned booths and paper ballots. No amount or technological tinkering can transform electrical impulses into a tangible paper trail. The evidence suggests that internet voting will expose the American electoral system to unprecedented levels or fraud, to such an extent that voting could in time become corrupt and compromised beyond repair. Internet voting is a bad idea whose lime has not come, and quite possibly never will. Paper balloting, election monitoring that is open to the public, and other traditional electoral safeguards (including, in the case of machines, the generation of a paper trail) have served us well for many generations. In spite of its flaws, the American system of voting remains the most reliable in the world.

This article was co-authored by Steve Bonta