

PRESS RELEASE

July 24, 2003

ELIMINATING COMPUTER VOTING SYSTEMS

By Harry Braun

According to an article "Computer Voting is Open to Easy Fraud, Experts Say," written by John Schwartz and published in The New York Times (July 24, 2003), the software that runs many of the high-tech voting machines contains serious flaws that allows voters or poll workers to alter ballots and election outcomes without being detected. According to Dr. Aviel D. Rubin, the technical director of Information Security Institute at Johns Hopkins University who participated in the evaluation of the software developed by Diebold Elections Systems that is used in over 33,000 computer voting machines in the U.S., "We found some stunning, stunning flaws."

According to Dr. Adam Stubblefield, one of the study's co-authors, even though such systems issue computer-chip bearing "smart cards" to voters, anyone with \$100 worth of computer equipment could allow people to produce these smart cards that would allow them to vote as many times as they like. The list of flaws in the in the Diebold software is long, according to the paper, which is online at <http://avirubin.com/vote>. Indeed, according to the study, ballots could be easily altered by anyone with access to the computer voting machines.

Y2K

The unnerving aspect of relying on computers and computer experts is that no one really knows for sure how well the systems are working, or how such systems could be impacted by hackers. Indeed, during the period leading up the Y2K issue, none of the best and brightest computer experts could predict what would happen as the year 2000 arrived. This uncertainty resulted in literally billions of dollars being spent by American companies and the military on dealing with potential computer problems that never existed in the first place. While computers are now critical to operating many aspects of our civilization, their susceptibility to software fraud makes them unacceptable as the basis for electing candidates to public office.

Paper Ballots

Democratic institutions are far too important to be left to chance, particularly when it involves dealing with the highly technical "black art" of computer software hackers. Nor are such risks necessary. Paper ballots were used when the American democracy was founded in 1776, and many countries, such as Canada, still use paper ballots for citizens to vote for candidates in national elections. As a result, Canadian officials have not had the embarrassing election confusion and delays that have characterized computer-dependent elections in the U.S. By returning to the use of traditional paper ballots, a hard copy of the voters selection is created that can always be recounted in the event of a close election. This would eliminate the many potential ways for computer hackers to manipulate the outcome of elections in the U.S. Voting is a sacred practice that must be free of such corruption. To comment on this subject of eliminating computer voting systems in the U.S., please send your thoughts to b@democracyamendment.us or call (602) 977-0888.