

What do the Experts Say?

“Only real recounts (cross-checking paper records against official tabulations), not just rereading machine totals, will resolve close elections.” October, 2006 *The American Statistical Association*
<http://www.amstat.org/news/StatisticalIssuesInElections.pdf>

“Computer viruses ... can spread malicious software automatically and invisibly from [Diebold] machine to machine during normal pre- and post-election activity” and “even careful forensic examination of these records will find nothing amiss” “anyone who has physical access to a voting machine or to a memory card can install said malicious software in as little as one minute.” “some of these problems cannot be remedied without replacing the machine’s hardware.” *Princeton University Computer Scientist Ed Felten* <http://itpolicy.princeton.edu/voting/>

“Technicians or election officials could be producing infected memory cards without any knowledge of what they were doing.” “We’ll never have secure machines if the vendors succeed in keeping the inner workings of their machines secret from the security experts.... Secrecy is not the road to security.” “The Princeton report describes two attacks: a vote-altering attack and a Denial-of-Service attack” *Yale University Computer Scientist Dr. Michael Fischer*
<http://www.verifiedvotingfoundation.org/article.php?id=6387>

“The current generation of electronic (DRE) voting machines are not secure, do not provide voters with a way to know that their votes are being tabulated correctly, and do not provide a mechanism for effective recounts when errors arise. As such, they represent an unacceptable technical risk, regardless of how people feel about them.” *Brigham Young University & University of Utah Computer Scientists (Carter, Windley, Brundvand, Gopalakrishnan, Hanscom, Jones, Lee, Regehr, Seamons, Shirley, Drake)* http://utahcountvotes.org/voting_system_advice.pdf

“The basic problem of e-voting can be understood without an in-depth knowledge of computer technology. Here is a helpful analogy: Suppose voters dictated their votes, privately and anonymously, to human scribes, and that the voters were prevented from inspecting the work of the scribes. Few would accept such a system, on simple common-sense grounds. Obviously, the scribes could accidentally or intentionally mis-record the votes with no consequences. Without accountability, a system is simply not trustworthy, whether or not computers are involved. “ and “You don't need a Ph.D. in computer science to understand the basic problem with computerized voting. Computer systems are so complex that no one really knows what goes on inside them. We don't know how to find all the errors in a computer system; we don't know how to make sure that a system is secure or that it hasn't been corrupted (possibly even by its designers); and we don't know how to ensure that the systems in use are running the software they are supposed to be running.“ *Stanford Computer Scientist David Dill* <http://www.verifiedvoting.org/article.php?id=5789>

“Diebold’s system is utterly unsecured. The entire cyber-security community is begging them to come back to reality and secure our nation’s voting.” *Pentagon Cyber-Security Advisor Stephen Spoonamore* <http://abcnews.go.com/WNT/Technology/story?id=2596705&page=2>

“We conclude that this voting system [Diebold] is unsuitable for use in a general election.” *Johns Hopkins University Professor of Computer Science Avi Rubin in a paper presented at the 2004 IEEE Symposium on Security and Privacy.*

“There are no standards. There is no scientific research ... there’s an erosion of voting rights implicit in the inability to trust the technology that we use and if we were another country being analyzed by America, we would conclude that this country is ripe for stealing elections and for fraud.” **DeForest Soaries, Former US Election Assistance Commission Chairman 2004-2006 (appointed by Bush)**

“Many of the hard drives and apparently all of the motherboards of the voting machines are Made in China. China is known to be attacking the Dept of Defense, Commerce Dept and other government computers. The motherboard controls the computer and hiding a malicious program in the boot sector of a hard drive isn’t much of a trick, one has to assume that some or all of the Diebold voting machines are potentially, even probably controlled by China (Security 101).” And “Diebold is based on Microsoft Windows. No other operating system in the world is as subject to so many viruses, Trojan horses, hack tools, worms, or other attacks..” and “Diebold has repeatedly used uncertified and untested software and hardware in elections, making a mockery of even the weak certification and testing procedures in place.” And “Diebold has repeatedly failed to correct known security flaws and software bugs.” and “It has become easy to determine that a Diebold representative is dissembling. His, or her lips are moving.” **Dr. Charles Corry, Colorado Springs, CO, former IEEE (the Institute of Electrical and Electronics Engineers) member of the voting system guidelines committee for 4 years (& former Marine corporal) October, 2006**

“Some believe that computer touch screen machines are the future of electoral systems, but the technology simply fails to pass the test of reliability. As anyone who uses one can attest, computers break down, get viruses, lose information, and corrupt data. We know this to be the case, and so we back-up our files to ensure nothing important is lost. Paper ballots serve as the ultimate back-up for our elections, providing secure and permanent verification of the will of the people...When a vote is cast, a vote should be counted. With paper ballots we will have a record. With paper ballots the fundamental principle of one person, one vote is safe.” **Democratic Governor Bill Richardson – NM**
<http://utahcountvotes.org/US/GovRichardsonLtr20060301.pdf>

Maryland Gov. Robert L. Ehrlich Jr. (R) called for the state to scrap its \$106 million electronic voting apparatus and revert to a paper ballot system for the November [2006] election. "When in doubt, go paper, go low-tech," he said. Ehrlich advocated leasing optical scan machines that use paper ballots... **Republican Governor Robert Ehrlich – MD** Washington Post Thursday, September 21, 2006
<http://www.washingtonpost.com/wp-dyn/content/article/2006/09/20/AR2006092001356.html>

“All three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections.” and “Few jurisdictions have implemented any of the key countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.” **The Brennan Center (NYU Law School)**
Experts include statistical consultant, professor University of California at Davis; Electronic Privacy Information Center; professor Stanford University, PhD, Cyber Defense Agency LLC; former CEO of F-Secure PLC; Lawrence Livermore National Laboratory and Chair of the California Secretary of State’s Voting Systems Technology Assessment and Advisory Board; prof. University of Iowa; PhD NIST; PhD, NIST; prof. MIT; Former Chief Security Officer, Microsoft and eBay; Counterpane Internet Security; PhD, formerly of the Computer Science; Artificial Intelligence Laboratory at MIT; prof. University of California at Berkeley; prof. Rice University; Electronic Frontier Foundation
<http://www.brennancenter.org/programs/downloads/SecurityExecSum7-3.pdf>

“It seems that integrity and honesty aren’t terribly important at Diebold...” and “We send people to death row on flimsier and more circumstantial evidence...” “How much are you willing to pay for secure trustworthy elections?” “What more would these machines have to do to prove they’re dangerous, whistle Dixie while they miscount our votes?” **Andrew Kantor, technology writer for USA Today, former editor PC Magazine and Internet World.**
http://www.usatoday/tech/columnist/andrewkantor/2006-09-29-diebold_x.htm