SHOULD COMPUTERS BE USED FOR VOTING?

I have been involved in computerized voting systems for 27 years, having been an official examiner of electronic voting systems for various states since 1980, conducting more than 120 such examinations, and testified on voting issues before the U.S. Congress four times and before state legislatures five times. So I have learned a few things. First, computers afford the most secure methods of voting ever developed, and computers can guide voters through the process of voting much better than any instructions that might be printed on a paper ballot. But I have learned something else: the public does not trust computers, or the people who programme them enough to rely on electronic methods of voting. At least that is true in the United States.

The U.S., unlike many countries, has very complicated ballots. In one county in California in 2006 there were 30 races on the ballot involving 98 different candidates plus another 30 referenda to be voted on. It required voting on six sides of optical scan sheets. Unfortunately, the U.S. experience with electronic voting has not been good. Ever since the Buchanan debacle of 2000, which resulted in the bungling of punched cards, every other method of voting has led to problems. Most recently, in an election in Sarasota County, Florida, more than 18,000 voters failed to cast a vote for a critical legislative race, a virtually unprecedented undervote of 15%.

Even when there is no overt irregularity, commercial voting machines have shown themselves to be among the least reliable devices on this planet. It has been reported anecdotally that approximately 10% of electronic voting machines fail in some respect during the average of 13 hours they are in use on Election Day. In some cases the experience is much worse. Unfortunately, such a failure rate is actually permitted by applicable government standards, although such a consequence was never intended. The machines are allowed to exhibit a mean time between failure (MTBF) of 163 hours. An ordinary personal computer has an MTBF of about 30,000 hours, almost 200 times better.

The result of the U.S. experience is that Congress and the states are moving to outlaw electronic voting and replace it with either hand-counted or optically scanned paper ballots. That will be a great mistake, for it ignores the very reason voting machines were introduced in the first place - to eliminate rampant corruption of elections through manipulation of paper ballots. In a paper ballot system, there is only one copy of the voter’s choices. If anything happens to that copy, such as alteration, mutilation, loss, or augmentation (called ballot-box stuffing), it is impossible to reconstruct the voter's original choices and the election is permanently compromised. Many countries exhibit an inglorious history when it comes to ballot manipulation. In contrast, modern electronic systems keep redundant encrypted ballot records on multiple physical media. It is essentially impossible to corrupt all of them in a consistent fashion, making it easy not only to detect any attempt to intrude, but allowing easy reconstruction of the election.

Instead of expending engineering effort to improve system reliability and hence public comfort, the U.S. is poised to move backward. The reason is largely unwarranted fear, compounded by computer scientists who know a lot about computer security but very little about security of paper records. I urge a serious, scientific, comparative study of the common methods of voting with a view toward improving the best modern system rather than discarding them.

For further reading: