Online voting: An open invitation to voting fraud

Internet voting systems are not secure and they don't live up to their promise to increase turnout either

BY CRISTIAN WORTHINGTON, VANCOUVER SUN MAY 10, 2011

The Internet voting system approved by Vancouver city council promises unprecedented and untraceable voter fraud if it is allowed to proceed, writes Cristian Worthington.

Photograph by: Mario Anzuoni, Reuters

The Internet voting system approved by Vancouver city council promises unprecedented and untraceable voter fraud if it is allowed to proceed. We can only hope the provincial government will have the good sense to reject the city's plan.

On the face of it, the system would allow voters to cast their ballots from the comfort of their own home. The idea sounds attractive and inevitable. After all, isn't everything going online?

Proponents suggest Internet voting will increase voter participation and will be secure. They are wrong on both counts.

Voter participation has been dropping for decades. The downward trend predates the Internet. Early trials of Internet voting systems have seen negligible increases in participation (two or three per cent) which can probably be attributed to the novelty factor.

Those who assume Internet voting will attract youth voters need only look at the turnout for Monday's federal election. It was the third lowest in history. All the hype about the youth vote being driven by social media and "vote mobs" did not translate into waves of youth voters. Otherwise, we would have seen a higher total vote.

Internet systems are secure enough for banking, so you might think Internet voting systems are up to the task of collecting and counting votes.

Unfortunately voting systems are different from online banking. Banking systems have audit trails that link the identity and conduct of a user. A voting system cannot link your name to your vote because the ballot must be secret. There is no way to determine whether a fraud has occurred or who committed it. This means that a candidate is deprived of the right to challenge results and have a recount. Internet voting systems presume that everything and everyone involved is beyond reproach.

Banking systems accept a level of fraud. If a banking customer observes a fraud the transaction can be reversed. A voting system does not offer the voter the ability to posthumously examine a vote and does not afford officials the option of correcting an error.

The current paper ballot system is not perfect either. A person can commit a single instance of fraud by showing up at a voting station pretending to be someone else and casting a ballot. But this requires a false ID and the risk of arrest.

It's much easier to commit fraud on an Internet voting system. A voter can be coerced to vote for a specific candidate or sell his/her PIN number to a third party. In these cases there is no significant chance of arrest because the voter is at a remote location.

Systemic fraud (fraud on a system wide scale) is difficult with the current paper ballot system. If you voted on Monday you will recall the little strip torn off your ballot by the poll clerk. The strip ensures the number of ballots placed in the box equal the number of ballots issued by the officials at your poll. This prevents ballot box stuffing.

When the poll clerk handled your ballot before you placed it into the box you were being prevented from leaving the poll with a blank ballot and starting a scam called the "floating ballot." You were prevented from starting a chain of voters entering the polling station with a prefilled ballot and getting paid for returning with the next blank ballot in the chain.

A large scale fraud is much easier on an Internet voting system. Hackers can break into the server and change votes or launch "denial of service" attacks that disrupt voting. Unlike a paper based system these acts can be perpetrated by someone thousands of kilometres away and impact thousands of votes.

While it is reasonable to assume the servers hosting the voting system will be relatively secure, we cannot say the same for a voter's computer.

Hackers can infect a voter's computer with a virus that will observe or change the voter's vote. The chief electoral officer has no way of certifying the quality of security on your home computer.

Biometric or other security schemes could be used to ensure the identity of the voter, but none of these technologies are cost effective or in wide use.

The case for Internet voting is weak and we cannot afford to overlook the risks. In 1992 I witnessed how badly things can go when I was called in as a trouble shooter by the Liberal Party of Nova Scotia after the first telephone voting system ever used in Canada had a catastrophic failure. The vote had to be postponed until the following week.

In considering Internet voting systems the question we all need to ask is: If it all goes terribly wrong is the electorate ready for the prospect of a do over?

Internet voting may have legitimate uses in applications like party nomination meetings, where the benefit of having all party members participate is seen to outweigh the risks of fraud. But the prospect of having the mayor of Vancouver elected by a hacker is unthinkable.

Cristian Worthington is the owner of several technology firms. He was the first to conduct a computerize enumeration of a federal riding in Canada and the first to install riding management software in the offices of federal MPs. He has lectured on Internet voting systems.