Brief for the Special Committee on Electoral Reform
Geoffrey Glass, 7 October 2016

I urge the Committee to reject online voting. Online voting suffers from insurmountable security weaknesses that open the door to the potential for massive undetectable election fraud. It shuts the public out of taking responsibility for and witnessing the election process, instead forcing them to rely on the authority of experts. Even if an election is in fact fair, it undermines legitimacy. This is close to my expertise: I have a doctorate in communication with a focus on technology, a degree in computer science and long experience with Internet software development. I volunteered as a scrutineer in the 2015 federal election.

Online voting (indeed any computer voting) would be a terrible mistake. So long as we have secret ballots, an online voting system can never be secure. Moreover, even with a secure system, public trust must rely on faith in experts.

A thought experiment illustrates the problem. The current process of voting, involving paper ballots, cardboard boxes, and hand counts, can be broken into stages. What seems straightforward for paper rapidly becomes complex when a machine is involved.

First, the voter makes her choice and uses a pen to mark it on a paper ballot. She can visually verify that the vote has been recorded correctly.

Second, the voter places the ballot in a box. So long as the box remains unmoved and unopened, she knows that the vote is included and has not changed.

Third, election officers open the box, sorts the ballots, count them (in part to check that no ballots have been added or removed), and re-seals them in the box.

Fourth, officials obtain the record of the count and report it publicly.

Computers introduce complexity and risk at every step in this process, but I will focus only on the first. Imagine that instead of computerizing the whole system, we simply replace the pen in step one with a machine in a black box. Instead of marking a paper ballot, the voter presses a button. The machine lights a bulb indicating her choice and produces a sealed envelope with the ballot inside. She takes the envelope to the ballot box and the process continues as before.

How can the voter confirm that the mark on the ballot in the envelope is correct? Not by inspecting the ballot: like the signal in a computer's memory, it is hidden. Not by the lit bulb: it is supposed to show which box was marked, but whether it actually does so depends on hidden wiring. Not by inspecting the machine: to prevent tampering, it is sealed. Not by asking elections officials to do any of these things: like the voter, they have no access to the workings of the box.

The only people who can reassure the voter that her vote was marked correctly are experts not even present at the poll: the designers, manufacturers, and installers of the box. If any one of them is incompetent or dishonest, or if anyone else has had access to the box, it (and others like it) could be compromised. At a polling station, only one of the people present can commit fraud, while everyone else who is present has the opportunity to observe and prevent it. For the machine, anyone who ever touched it is a risk, and may have the opportunity to do so alone and unobserved.

Some computer scientists suggest that mathematical techniques could (potentially, at some point in the future) guarantee the correctness of software for storing and tabulating votes. Maybe so. But as any user of software knows, there is a big difference between the possible and the actual. Regardless, math is just part of a voting system. Even if steps two and three above are 100% secure and bug-free, what about steps one and four? No algorithm can guarantee correctness at the interface with human beings, or the mass of consumer hardware, operating systems and browsers used by potential online voters. To commit fraud, all that is necessary is to deceive voters about their choices, or fool elections officials about the results. Any technique for validating the process creates the need to trust yet another black box.

Of course, elections are hardly perfect. As a scrutineer, it was clear to me that our procedures are not air-tight. Fraud happens, but I believe it seldom has any impact on the result. Aren't a few weaknesses a fair price to pay for more accessible, inclusive elections?

No: when computers are involved, compromising on one machine could mean compromising all of them. Fraud at the ballot box is bound to be small scale and confined to a single poll: a partisan "helping" an elderly man to mark his ballot; an official sneaking a handful of extra photocopied ballots into the box (when photocopies have been allowed). Access to a computer could mean affecting every vote cast; access via the Internet could mean influencing many ridings. Anyone on the Internet might attempt to hack the system; in the case of a national election, the potential rewards for doing so are huge.

On its own, even this is manageable: if we know there is a problem, we can take steps to address it. But when fraud does happen, it is liable to be undetectable. Code that deletes votes can erase itself from the record. Internet commerce possible is possible not because the Internet is secure (far from it), but because failures are evident. When I buy a product on Amazon, I can check my credit card statement to see that I was not overcharged, just as Amazon can check their payments to see that they really received the money. Not so with voting. When a secret ballot goes into a computer, I can only hope that it is counted. When fraud can be detected, it can be managed. When it is undetectable, it cannot.

Finally, there is the problem of trust. Regardless of what you think of Bush v. Gore, the polarization aroused by hanging chads tore American society apart. The anger still has not gone away; it continues to divide the country. Not only must elections be fair; they must be seen to be fair.

Assume for the sake of argument that I am wrong: that the technology really can be made secure. How do you convince me that I am mistaken? How do you show me that the system is secure? Unless I am an expert in all the relevant technologies and processes, you cannot explain to me how the system works. All you can do is ask for my trust, and present me with experts and authorities who claim that it is correct. Will I believe them? Only if I am convinced that they are trustworthy and capable of ensuring fairness. I have a computer science degree and I have been programming the Internet for 20, and I am suspicious. How will other citizens respond? In a hotly contested election, people look for excuses to reject the outcome. Given concerns like those I have described, they will be hard to convince.

This is more than a practical point. Fundamentally, democratic elections are about citizens taking responsibility for our own governance. To replace a process that anyone can observe and understand with one that we cannot, and instead tell us to place our faith in authorities and experts, is to take the process of selecting a government away from the citizens. It is profoundly undemocratic.

Your committee is charged with seeking reforms that increase public confidence in the legitimacy of elections. I strongly support your goals. But while I am an advocate of proportional representation, I do not wish to distract from a far more important issue. My recommendation is simple: Canada should continue to use physical paper ballots and proven election procedures that can be witnessed, carried out and proven correct by ordinary citizens.

Sincerely,

Geoffrey Glass

Burnaby, BC