Richard Akerman
Submission to the Special Committee on Electoral Reform
An evaluation of online and electronic voting for Canadian national elections

Section 1: Summary

Executive Summary

The use of online voting or electronic voting machines would greatly increase risks, without bringing sufficient benefits.

Considerations:

- Widespread use of online voting would enable widespread coercion of voters, including vote buying.
- The innumerable software and hardware components that would be involved in marking, transmitting, receiving and counting an online ballot represent an unreasonably high risk to the chain-of-custody for the ballot.
- Canadian government departments have already been successfully cyberattacked by nation-states.
- Computer security experts warn that online voting is not secure.
- National security experts warn that online voting is not secure.
- Social science evidence indicates that online voting won't increase turnout.

For these reasons, the Special Committee on Electoral Reform should recommend against the use of online voting and electronic voting in Canadian elections.

Evaluation Against Principles

1. **Effectiveness and legitimacy**: without any paper ballots to count, accusations of voting system hacking may allow the legitimacy of the election to be called into question.
2. **Engagement**: online voting does not significantly increase voter turnout, and is primarily used by voters who would have otherwise voted in a polling place.
3. **Accessibility and inclusiveness**: online voting will introduce both visible and hidden technological complexity and exclude those without good Internet access.
4. **Integrity**: the security risks introduced by online and electronic voting are so great that the Australian Parliament has categorized the risk to integrity as catastrophic.
5. **Local representation**: electronic and online voting have no implications for local representation.

Section 2: Considerations and Recommendations

Remote Voting Considerations

The process of marking a ballot alone and unobserved behind a voting screen in a polling place did not arise by chance; it is a specific design choice intended to reduce the risk of coercion.

Coercion means that someone is influenced to vote for a particular party or representative, either through rewards (e.g. social approval, vote buying) or through threats (e.g. threats of violence or employer threats to their job). The risk of coercion has existed throughout the history of voting.

When someone other than the voter can see the ballot being marked, or the voter can prove to a third party how they voted after the ballot has been cast, the risk of coercion becomes very high.

Therefore almost any remote voting system, including online voting, brings with it an increased risk of coercion.

Additionally, remote voting introduces risks to the **chain-of-custody**. The chain-of-custody is an election integrity requirement, where individual ballots and collections of ballots are always in safe custody and under observation. The observers should be drawn from opposing political factions, in order to ensure that there isn't any collusion in altering ballots.

The outcome of a strong chain-of-custody is that, once cast, individual ballots are kept safe from alteration or loss, and the total collection of ballots (e.g. in a ballot box) is similarly protected, included from the addition of ballots not cast by electors ("ballot stuffing").

Online voting may seem as if it has a very short chain-of-custody, from the computer through the Internet to the voting server, but this is a misunderstanding of the actual steps involved in casting a ballot over the Internet. The actual chain-of-custody, the "hands" through which an Internet ballot passes on its way to being counted, is almost innumerable. The voting software, the web browser, the operating system, other applications on the computer, network devices, and layers of software on the central voting server all could interfere with the ballot, altering it or discarding it, or indeed adding additional ballots. In a very real sense, the chain-of-custody for an online ballot is everyone who has ever written any of the millions of lines of software in the operating systems, applications and network devices that will process the digital ballot. It is a simply incredible extension of trust to a huge number of strangers. For this reason, the risk to the chain-of-custody for an online vote is extremely high.

Technological Voting Considerations

The introduction of computer technology into the voting process can seem, at first glance, to bring with it great convenience and efficiency. However, a more detailed examination of the unique characteristics of the voting process reveals that computer technology does not meet all of the necessary requirements for auditability and security; paper and pencil are in fact the appropriate technologies.

Auditability, the ability to demonstrate that the votes have been correctly counted, is critical to public confidence in elections. When elections are highly contentious, it is vital to be able to demonstrate to all political factions that the votes have been properly counted. Counting paper ballots in public with observers from all political parties in an excellent, easy-to-understand method that provides a clear, transparent count. Upon a close result, the ballots can be sent to a judicial recount for final decision.

Contrast the public paper ballot count with a paperless electronic voting machine or online voting count, in which the count is simply produced out of the black box of the computer. There is no visible evidence other than a number on a screen. There is no meaningful possibility of recount; there is nothing to recount. This is not because the computer is a perfect counting machine; it's because there is simply no additional evidence that can be examined other than what is already inside the computer. And what is inside the computer could have been manipulated by attackers in many different ways.

This brings us to the issue of **security**. The online world is one that is full of threats, and threats that differ from the physical world. In Canada's current paper-based, physical location, hand-counted election, there are over 60,000 polling stations where ballots are counted. To interfere with the casting or counting of ballots at polling stations at a large scale, large numbers of people would have to be physically present in the polling stations, taking great risk in an environment where there are multiple observers from opposing political factions.

In contrast to the physical world, the online world brings three new capabilities to attackers:

1. Distance
2. Automation
3. Scale

An online attacker, in an attempt to disrupt an online election, does not even need to be in the same country. They can attack from a **distance**, and even in cases where attacks have been attributed to nation-states, we see that there are often minimal consequences for such attacks.

Additionally, an online attacker can take advantage of the power of the computer for **automating** tasks. In fact, automated scans for computer vulnerabilities run continuously on the Internet, discovering systems to compromise. The software in these systems can embody some of the most sophisticated computer attack knowledge of experts from around the world,

while running with the press of a button. This means even a single attacker can deploy very sophisticated attacks.

It is important not to imagine this as a single individual sitting at a single computer, attacking a single other computer. Automation and widespread inexpensive computing capacity means that attacks can take place at **scale**. This could be a single computer simultaneously attacking many other computers, but in practice is actually many computers (sometimes thousands of computers, in a "botnet") attacking either a single target, a small set of computers or thousands of other computers. This might be with the goal of intrusion, but it might also be simply a "denial of service", in which the target computer systems receive so many requests they cannot function properly.

Since an election cannot be re-run, even a denial of service (which is a very simple attack) could be catastrophic on election day. More sophisticated attacks, including ones that compromise the voting systems and alter votes, could be even more devastating, particularly if the attack is not discovered until months after the election.

Recommendations

- Slow down; there is no need to rush the process of analysis for deciding about online and electronic voting.
- Online voting is a subject for computer science research, not for trials. As Chief Electoral Officer Mayrand requested the committee provide directions for research, convene an expert committee of computer scientists to define a research program. This research could support addressing the challenges related to the principles of legitimacy, accessibility and inclusiveness, and integrity raised earlier.
- The expert committee of computer scientists might consider directing research in the following areas:
    - How to reduce the risk of coercion when using remote voting
    - How to improve the chain-of-custody when using online voting; how provide an end-to-end verifiable vote
    - How to provide adequate security measures for online voting, in an environment of insecure citizen devices and sophisticated nation-state attackers
- Electronic voting machines (including vote counting technology) must be understood as electronic voting *computers*; they bring risks of attack that are similar to online voting. They are also a subject for research, not for trials.

- One very immediate approach to examining online voting would be to have Canadian researchers, with accompanying legal protections (overriding any claims of intellectual property protection), inspect in detail and in public all online voting systems currently being offered in Canada.

- Should the government decide at any time to proceed with developing online voting and/or electronic voting computers, all development must be in public, using open source, in alignment with the principles of open government. Key characteristics of such open development include:
    - Permit inspection and testing of all voting-related code by the public at all times.
    - Ensure that the law permits any security investigator (including a member of the public) to conduct tests against electronic and online voting systems, including systems from third parties.
    - If third-party technology (e.g. from for-profit corporations) is used as part of online voting or electronic voting machines, do not permit the shielding of inspection of that third-party technology due to claims of intellectual property concerns. There is no security through obscurity.
- Before proceeding with technology deployment, the government must fully cost the entire lifecycle of any technology being used, including maintenance, updates, physical storage and facilities.

Section 3: Supporting Evidence

Coercion

Minister Maryam Monsef was eloquent on the issue of coercion. At the Online Voting Roundtable on September 26, 2016, she stated “Also, how do we know that the individual clicking… their vote online isn’t being forced, maybe it’s a partner that is violent or coercive in some way. Maybe it’s an individual with accessibility or disability or exceptionalities and they’re being persuaded by someone else to vote a certain way. How can we make sure that that integrity of the vote, the secrecy of the vote, is maintained?”. (Monsef, 2016)

In his TEDx presentation “Internet Voting? Really?”, Andrew Appel describes the history of voting in the United States, starting with the original voting method of simply saying the vote out loud, in public. He makes it clear that the secret ballot and associated polling station privacy procedures were specifically designed in order to reduce the risk of coercion. (Appel, 2016)\

Chain-of-custody

In a video for Computerphile, Tom Scott vividly describes the chain-of-custody issue, saying “Would you be happy … just calling someone up on your phone, telling them your vote, but they promise to keep it secret, and at the end of the election, all those people who have been sitting on their own phone up one other person in private and tell their results, and then that final person – who promises to count it all up accurately – just announces who’s won. Because that is essentially what electronic voting is.” (Scott, 2014)

Canadian Government has been successfully cyberattacked

There are two major sets of successful attacks on Canadian government departments that have been reported. The first, in 2011, compromised the Finance Department, Treasury Board Secretariat, and Defense Research and Development Canada. (Weston, 2011) (Ljunggren, 2011) The second, in 2014, compromised the National Research Council. (Barton, 2014) (Treasury Board of Canada Secretariat, 2014) (Freeze, 2016)

Computer security issues

The literature about the computer security issues related to online voting and electronic voting is so extensive, with so many statements by computer scientists recommending against online voting, that it would take an entire separate briefing report just to do it justice. Fortunately, Eric Geller has written such a report, entitled “Online voting is a cybersecurity nightmare”. (Geller, 2016) From a more academic angle, computer security expert J. Alex Halderman has a book chapter “Practical Attacks on Real-world E-voting” that describes in detail the real (not theoretical) flaws in various electronic and online voting systems. Most notably in the section on Internet voting, he reports on how the Washington, DC system was hacked when outside

researchers were invited to probe its security before the election, and the many flaws in operational security found with Estonia's Internet voting system when outside researchers were invited to inspect it. (Halderman, 2016)

There is also a statement about Internet voting available from the US Association of Computing Machinery, the largest organization of US computer science professionals. It concludes: "systems need some means of preserving the ability to audit and/or recount the votes. At the present, paper-based systems provide the best available technology to do this." (US Association of Computing Machinery, n.d.)

Warnings from national security experts

Neil Jenkins of the US Department of Homeland Security has stated "… online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results." (Horwitz, 2016)

US Homeland Security Secretary Jeh Johnson has stated "These [cybersecurity] challenges aren't just in the future -- they are here today. … In a few cases, we have determined that malicious actors gained access to state voting-related systems." (Johnson, 2016)

Turnout including youth turnout

The City of Kitchener's 2012 report on Internet voting finds that "There is clear evidence that, regardless of geography internet voting does not attract younger voters." (Gosse, 2012) Similarly, the 2014 BC Independent Panel on Internet Voting finds in their report that "research suggests that Internet voting does not generally cause nonvoters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have already decided to vote." (Archer, Beznosov, Crane, King, & Morfitt, 2014)

Examples of conclusions about online voting in other countries

Just to cite three examples, the UK and Norway stopped online voting after trials, due to security and other concerns, while Australia, after conducting an extensive Parliamentary Committee inquiry, concluded their nation was "not in a position to introduce any large-scale system of electronic voting in the near future without catastrophically compromising our electoral integrity." (Glover & Branigan, 2005) (BBC News, 2014) (Parliament of Australia - Joint Standing Committee on Electoral Matters, 2014)

Works Cited

Appel, A. (2016, March 26). *Internet Voting? Really? | Andrew Appel | TEDxPrincetonU [Video file]*. Retrieved from YouTube: https://youtu.be/abQCqIbBBeM

Archer, K., Beznosov, K., Crane, L.-A., King, V., & Morfitt, G. (2014, February 12). *Recommendations Report to the Legislative Assembly of British Columbia.* Retrieved from British Columbia Independent Panel on Internet Voting: http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

Barton, R. (2014, July 29). *Chinese cyberattack hits Canada's National Research Council*. Retrieved from CBC News: http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

BBC News. (2014, June 27). *E-voting experiments end in Norway amid security fears*. Retrieved from BBC News: http://www.bbc.com/news/technology-28055678

Freeze, C. (2016, September 2). *Canadian research body relied on paper communications after Chinese hack, documents show*. Retrieved from Globe and Mail: http://www.theglobeandmail.com/news/national/records-show-extensive-fallout-from-chinese-hack-of-national-research-council/article31695327/

Geller, E. (2016, June 10). *Online voting is a cybersecurity nightmare*. Retrieved from The Daily Dot: http://www.dailydot.com/layer8/online-voting-cybersecurity-election-fraud-hacking/

Glover, J., & Branigan, T. (2005, September 7). *E-voting plans shelved after extensive trials*. Retrieved from The Guardian: https://www.theguardian.com/technology/2005/sep/07/egovernment.politics

Gosse, R. (2012, December 10). *FCS-12-191 - Alternate Voting - Internet Voting.* Retrieved from City of Kitchener - Laserfiche WebLink: http://lf.kitchener.ca/uniquesig0d1d2aa1a38f6e69dc1e79e99d780c34f537a34d9c901a0d7cbb1976cbfdd057/uniquesig0/WeblinkExt/0/doc/1235356/Page1.aspx

Halderman, J. A. (2016). Practical Attacks on Real-World E-Voting. In F. Hao, & P. Y. Ryan (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment* (pp. 145–171). CRC Press. Retrieved from https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

Horwitz, S. (2016, May 17). *More than 30 states offer online voting, but experts warn it isn't secure*. Retrieved from Washington Post: https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/

Johnson, J. (2016, October 1). *Statement by Secretary Johnson About Election Systems' Cybersecurity*. Retrieved from US Department of Homeland Security: https://www.dhs.gov/news/2016/10/01/statement-secretary-johnson-about-election-systems-cybersecurity

Ljunggren, D. (2011, February 17). *Canada says cyber-attack serious, won't harm budget*. Retrieved from Reuters Canada: http://ca.reuters.com/article/topNews/idCATRE71G0RG20110217

Monsef, M. (2016, September 26). *Voting Reform: Online Voting Roundtable – Maryam Monsef [Video file]*. Retrieved from CPAC - Cable Public Affairs Channel - cpac.ca/en/electoralreform/ - Electoral Reboot: What you need to know as MPs consider

how you elect them!: http://www.cpac.ca/en/jwplayer/?params=ZXA9NDkwMjE5NTUmcD1odHRwJTNBJTJGJTJGd3d3LmNwYWMuY2ElMkZ3cC1jb250ZW50JTJGdGhlbWVzJTJGY3BhYyUyRl9yZXNvdXJjZXMlMkZfaW1hZ2VzJTJGc3RydWN0dXJlJTJGQ1BBLTk2MC03MjBfRGlnaXRhbEFyY2hpdmVfZW4uanBlZyZzaGFyZT0=&time=172.054

Parliament of Australia - Joint Standing Committee on Electoral Matters. (2014, November). *Second interim report on the inquiry into the conduct of the 2013 federal election: An assessment of electronic voting options*. Retrieved from Parliament of Australia: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Second_Interim_Report

Scott, T. (2014, December 18). *Why Electronic Voting is a BAD Idea - Computerphile [Video file]*. Retrieved from YouTube: https://youtu.be/w3_0x6oaDmI

Treasury Board of Canada Secretariat. (2014, July 29). *Archived - Statement by the Chief Information Officer for the Government of Canada*. Retrieved from Government of Canada: http://news.gc.ca/web/article-en.do?nid=871449

US Association of Computing Machinery. (n.d.). *Internet Voting*. Retrieved from ACM US Public Policy Council: http://usacm.acm.org/evoting/category.cfm?cat=30&E-Voting

Weston, G. (2011, February 16). *Foreign hackers attack Canadian government*. Retrieved from CBC News: http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618