OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Internet Voting – Privacy and Security Risks

Sean Murray
Director of Research and Quality Assurance
June 11, 2020

Introduction

"Every vote counts" is a truism that has rarely been better demonstrated than in Newfoundland and Labrador's 2019 Provincial general election. It was not until June 21, 2019 after a judicial recount that Jordan Brown was declared elected in Labrador West with a 2 vote margin of victory. Not only did this decide the winner of that particular district, but it meant the difference between a majority and a minority government, which significantly impacted how the province would be governed.

The above example illustrates the importance of having an electoral process that enjoys a high degree of public trust. The method by which we vote, however, brings with it certain attributes which can either facilitate or potentially undermine voter privacy, which is a key foundation of that public trust.

This research has been prompted as a result of interest expressed at both the municipal and provincial levels in Newfoundland and Labrador in exploring the adoption of internet voting. In 2014 Municipalities Newfoundland and Labrador passed a resolution to request that the provincial government amend legislation so as to permit electronic voting. On February 25th, 2019 the provincial government announced the formation of an All-Party Committee on Democratic Reform. Included within the terms of reference released at the time was to make findings and recommendations on "changing or broadening methods to vote."[1] Media reports from the announcement interpreted this as a mandate to consider "allowing online voting."[2]

The purpose of this paper is to identify some of the privacy, security and related risks associated with internet voting. The literature on voting methods is vast and is an area of active and growing scholarship. In order to present an accessible and digestible paper, internet voting was chosen as an area of focus for several reasons. Chief among them is that there have already been initiatives to establish internet voting in Canada, interest has already been expressed in implementing it in Newfoundland and Labrador at least at the municipal level, and there has been significant scholarship and public debate around privacy concerns relating to internet voting.

Issues regarding other non-traditional voting methods have been the subject of ongoing public and scholarly debate for some time now, however it is not possible to include all of these within the scope of this paper. These include voting machines (typically touchscreen kiosks located in polling stations which have become common in the US) and mail-in ballots (currently in use in a number of jurisdictions, including the City of St. John's). Other issues regarding privacy in the electoral process have also been raised by Canada's Information and Privacy Commissioners, particularly in relation to the fact that political parties in Canada are generally not covered by privacy laws.[3] There are further issues relating to election integrity that extend beyond privacy which have been the focus of much research, however as this paper is issued under the auspices of the Office of the Information and Privacy Commissioner, it will primarily be limited to privacy issues associated with internet voting. Although these additional topics are out of scope in terms of the focus of this paper, they may be briefly referenced where the context requires it.

In Newfoundland and Labrador provincial elections are run by the Office of the Chief Electoral Officer (OCEO) and municipal elections are run individually by each municipality. All municipalities as well as

[1] https://www.gov.nl.ca/releases/2019/just/0225n02/
[2] https://www.cbc.ca/news/canada/newfoundland-labrador/democratic-reform-committee-1.5032826
[3] https://oipc.nl.ca/pdfs/FPT-SecuringTrustPrivacyInCanadasElectoralProcess-Resolution2018.pdf

the OCEO are public bodies subject to *ATIPPA, 2015*. As a result, any initiative to implement electronic voting may be subject to comment, audit or investigation by the Office of the Information and Privacy Commissioner to the extent that personal information may be collected, used or disclosed during the electoral process, and in particular whether the internet voting process, if implemented, meets the minimum security requirements of *ATIPPA, 2015*.

Under section 95(1)(e) of *ATIPPA, 2015* the Information and Privacy Commissioner may "engage in or commission research into anything relating to the purpose of this Act." The purpose of *ATIPPA, 2015* as stated in section 3 is to "facilitate democracy" by "ensuring that citizens have the information required to participate in the democratic process," secondly by increasing transparency and supporting accountability of public officials, and thirdly by "protecting the privacy of individuals with respect to personal information about themselves held by public bodies."

This paper finds that internet voting faces a unique and inherent conundrum: voting requires verifiability – the ability to confirm that the individual is who they say they are – and anonymity – the separation of the voter's identity from their vote once verification has occurred. The right to privacy and its relationship to political rights is central to this unique feature. Traditional voting using paper ballots achieves both requirements. With internet voting, in addition to the risk of cyberattacks and the loss of public trust that such attacks can engender, there are fundamental challenges in attaining both verifiability and anonymity which have not been overcome by internet voting proponents. While there may be benefits such as convenience associated with internet voting that should be considered, this paper finds that these benefits have not been adequately explored or demonstrated, nor that they would likely outweigh the known and unknown risks of internet voting.

The Secret Ballot: Some Practical Considerations

The secret ballot is a fundamental element of any functioning democracy. History shows that without it, the voting process can be neither free nor fair,[4] and in the past century there has been widespread adoption of the secret ballot in democracies throughout the world. In most cases it is a simple two-step process in which election officials confirm the eligibility of the voter before issuing a ballot. The voter then goes behind a screen so that no one else can see their voting choice, and the completed ballot is then placed in the ballot box. The entire process occurs under the supervision of electoral officials.

Clearly, privacy itself is a necessary element of the secret ballot. The voter is shielded from attempts to influence or strong-arm their voting decision. Any voting process that occurs outside of such a private yet supervised process may be subject to such attempts. It can easily be imagined that financial incentives can be offered or threats made to voters to make a certain choice if voting is to take place using a personal smartphone or home computer because the party doing the bribing or making the threat can force the voter to show the vote as it is cast. This is perhaps the more overt scenario where lack of privacy in the voting process can result in an illegitimate vote. At the time of writing, the United Conservative Party of Alberta is subject to an ongoing criminal fraud investigation by RCMP.[5] The Party

[4] https://www.heritage.nf.ca/articles/politics/history-of-vote.php "The first general election took place in the fall of 1832. There was no secret ballot. Individuals had to declare their vote in public at a polling station. This left voters vulnerable to intimidation or bribery. Fish merchants, clergy and others could easily use their influence to affect election outcomes."

[5] https://newsinteractives.cbc.ca/longform/inside-jason-kenney

held its leadership contest using online voting, and there are allegations that party members were solicited to provide their PIN number to one candidate's organizers who voted using those PINs. Whether or not there is a conviction, it is clear that confidence in that voting process has been shaken.

Other circumstances can be imagined where abusive relationships exist, in which a domineering individual in a household may either force another person to vote a certain way or may in fact impersonate them online by stealing the PIN number of other household electors. This could occur not just in spousal relationships but also in elder abuse scenarios, as well as any circumstance involving significant power imbalances in personal relationships. Victims in such relationships are rarely in a position to report such abuse to authorities for fear of reprisal, and in the immediate life priorities of such victims, having one's vote stolen may be the least of their worries. Furthermore, any such allegation would be very difficult to prove to the evidentiary standard required in a criminal prosecution.

Unique Characteristics and Unique Risks

Even considering some of the above-noted risks, many people continue to support internet voting, perhaps on the assumption that those scenarios are likely to be rare. I will therefore now focus primarily on the ultimate conundrum of internet voting, which involves recognizing the fact that casting a vote is unlike any other kind of online transaction. The act of voting in any secret ballot electoral system must have two characteristics: verifiability and anonymity. In other words, there must be a way to verify that each vote is a valid vote by an eligible voter, while at the same time guaranteeing that there is no record of which candidate the voter chose. One of the best layperson's summaries of the issue is found in an article in the *Daily Dot* by Eric Gellar, who interviewed a number of internet security experts including Stanford Professor David Dill:

> *Internet voting advocates often say things like, "If you can bank online, you should be able to vote online." But banks provide receipts for transactions, letting every party verify that deposited or withdrawn money went through the system correctly. You can ask your bank to investigate a bad transaction, just as your credit card company might call you to verify a suspicious one, but only because money tied to your identity is tracked through the global financial system.*
>
> *Unlike in banking, where fraud is detectable because money either lands in the appropriate place or disappears, and in paper voting, where physical evidence must be tampered with to rig the results, technology lets people do things while leaving literally no trace. "The system goes to great lengths to destroy the link between my name and the ballot that I cast," said Dill. "That's a property that's special to elections that almost no other system of electronic transactions deals with in the U.S."*

In the same article, Dill, as quoted by Geller, also referred to electronic voting machines. In terms of the underlying conflict of verifiability and secrecy, the problem faced by internet voting and by electronic voting machines is the same:

---

https://www.ctvnews.ca/politics/special-prosecutor-to-aid-probe-into-alberta-united-conservative-leadership-vote-1.4492502

"If you've got an electronic voting machine," Dill said, "somebody enters a vote, it displays the same vote, everything looks great, and then the voter says, 'Cast this,' the voting machine can change the record, either through errors or because of tampering, and there's really no way to detect that. Anybody who goes back to look at the electronic ballot will see a perfectly legitimate ballot which happens to be different from how the voter voted. And since the secret ballot demands that the link between the voter's identity and that cast ballot be broken, there's no way to go back and check."

As internet voting advocates point out, this problem is not unique to voting. Computers run stock markets, banks, schools, hospitals, charities, and defense contractors, and news websites. But in no other aspect of life besides voting does society demand complete anonymity. "The tricky bit for people to grasp," said Joe Kiniry, the research lead for Galois's verifiable-elections program, "is that the set of requirements around elections look and taste different than any other modern online system."[6]

Understanding the special requirements of voting, which are unique and different from any other kind of electronic transaction, is key to any assessment of the appropriateness of internet voting.

One leading expert in the field is Dr. Alex Halderman, Professor of Computer Science and Engineering and Director of the Centre for Computer Security and Society at the University of Michigan. His first major foray into this field occurred when the District of Columbia, to its credit, decided to run a mock election in order to allow outside parties to evaluate the security of its new internet voting system prior to the actual election. With only three days' notice, Dr. Halderman and his students were able to penetrate the voting system as he describes below:

- *We collected crucial secret data stored on the server, including the database username and password as well as the public key used to encrypt the ballots.*
- *We modified all the ballots that had already been cast to contain write-in votes for candidates we selected. (Although the system encrypts voted ballots, we simply discarded the encrypted files and replaced them with different ones that we encrypted using the same key.) We also rigged the system to replace future votes in the same way.*
- *We installed a back door that let us view any ballots that voters cast after our attack. This modification recorded the votes, in unencrypted form, together with the names of the voters who cast them, violating ballot secrecy.*
- *To show that we had control of the server, we left a "calling card" on the system's confirmation screen, which voters see after voting. After 15 seconds, the page plays the University of Michigan fight song.*

Yes, the system was easily hacked, but an even more important consideration is that election officials were unaware of the hack until voters began commenting on the little song that played every time they voted. Without this "calling card" the electoral officials may have considered the mock election a success and proceeded to hold the real election. Instead, Dr. Halderman explained to the officials how

[6] https://www.dailydot.com/layer8/online-voting-cybersecurity-election-fraud-hacking/

easy it was for his team to hack the system, and the District decided against proceeding with internet voting.[7]

Important work is also being done in Canada to study internet voting. Anthony Cardillo and Aleksander Essex of the Department of Electrical and Computer Engineering at Western University along with Nicholas Akinyokun at the University of Melbourne have recently released the first comprehensive study on the security of internet voting at the municipal level in Ontario.[8] The authors found numerous security failings in the execution of online voting in Ontario's 2018 municipal elections, and determined that the elections were operating without any province-wide standards. Security was entirely left to the individual municipality and the private vendor whose product was used to run the election. The paper details these security failings across all vendors and municipalities, however for the purpose of this paper it is noteworthy that the failure to protect privacy in the form of a secret ballot was one of the concerns expressed by the authors.

Some of the same issues that exist with mail-in ballots were identified by the authors, including people voting with the PINs of other voters. As noted in the paper:

> *Voting on someone else's behalf is an offense under the MEA* [Municipal Elections Act]. *Nevertheless, we heard anecdotal accounts from several independent sources of parents who voted on behalf of children living in another city, or people who voted on behalf of their spouse while they were at work. We also heard accounts of individuals gifting their unopened voter information packages to friends and family.*
>
> *Ultimately, knowledge of a PIN or date of birth does not establish a voter's identity. It merely establishes to the voting server that some entity on the other end of the connection knows a secret. Secrets, of course, can be transferred or intercepted.*[9]

While these issues exist with mail-in ballots as well, the scale of potential abuse for mail-in ballots is more likely to be smaller because of the distributed nature of postal mail, meaning that opportunities for fraud may be limited to within individual households or perhaps where there is a basis for coercion within social or familial circles beyond a household. Internet voting could also be subject to those fraud scenarios, but any activity conducted on the internet is also potentially susceptible to much larger scale hacking by actors with the intent to throw an entire election to one candidate or another rather than fraudulently cast a few votes.

Aside from the many issues identified with the integrity as well as the anonymity and verifiability of the electoral outcomes, it was also shown that, across all four vendors used by municipalities in Ontario, the researchers were of the view that it would be possible to re-identify supposedly anonymous voters and to learn how individuals voted, and therefore the secret ballot cannot be said to be an assured feature of online voting. Vendors using two factor authentication relied on both a PIN and the voter's date of birth. Because this information is transmitted to the voting server together with the voter's

---

[7] Dr. Halderman's technical paper is here: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf There are numerous videos and media interviews about the hack available online.
[8] Cardillo et al "Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?" https://whisperlab.org/ontario-online-E-Vote-ID.pdf
[9] Cardillo et al.

electoral choice, the authors conclude that this conflicts with the principle of ballot secrecy, because there are many ways to hack information in transit over the internet.

Having reviewed the litany of security issues associated with Ontario's 2018 online municipal election, the researchers found that with the many flaws, the lack of verifiability of the outcome and the increasing awareness among members of the public that the internet is a generally insecure medium, the most likely outcome over time was that online voting may eventually decline. They posited that at the municipal level internet voting would be less likely to be scaled back or abandoned because of hackers, malice or fraud. Instead, they expect that it will happen for a different set of reasons – essentially that enough flaws will come to light over time that the level of public trust necessary to sustain it will decline:

> *[P]urposeful, malicious interference, or fraud is not necessary to undermine an election. Nor is the honest discharge of an election sufficient to prevent it. Given enough time, a seed of doubt in an otherwise faithfully executed election may eventually grow to accomplish what even the best threat actor cannot.*[10]

Unlike in Ontario, the Province of British Columbia decided to proceed with greater deliberation when it chose to establish an Independent Panel on Internet Voting[11]. The Panel conducted a thorough review of considerations relevant to internet voting, consulting a wide range of experts and reviewing the use of internet voting in other jurisdictions. At the conclusion of its work, the Panel's number one recommendation in its 2014 Report was that internet voting should not proceed at either the municipal or provincial level. The Committee concluded that "[t]here are significant risks to implementing Internet voting that can jeopardize the integrity of an election, no matter the extent of implementation."

Another recent analysis of internet voting was completed by the House of Commons Special Committee on Electoral Reform, which issued its final report in December 2016. Although the report addressed a wide range of issues relating to electoral reform, a full chapter was devoted to consideration of online and electronic voting. The Committee conducted public consultations on the subject as well as hearing testimony from many witnesses. Although there was a degree of interest from the public in voting online, the security of the vote was a significant concern. The internet security experts who appeared before the Committee pointed out significant hurdles, including as noted elsewhere in this paper, the special requirements of verifiability and anonymity that are unique to internet voting in comparison with all other online transactions. The Committee noted concerns expressed about the transparency of the process as well:

> *A related concern regarding online voting is that it lacks transparency due to the absence of a paper trail. The paper trails produced through traditional ballots provides a simple backup system in the event that votes have to be recounted.*[12]

While there are examples of online voting proceeding without any reported incidents, it is important to understand that system errors and hacks that threaten the integrity of the result may not be detected. Sometimes a bug in security coding is not detected for many years after a system has been in use, or

---

[10] Cardillo et al.
[11] https://elections.bc.ca/docs/recommendations-report.pdf
[12] Chapter 6 – Online and Electronic Voting, Report of the House of Commons Special Committee on Electoral Reform https://www.ourcommons.ca/DocumentViewer/en/42-1/ERRE/report-3/page-267

never. Vulnerabilities can cause inadvertent, unnoticed errors, or they can open the door to hackers. Internet voting is especially susceptible to undetected problems because unlike other internet transactions, such as banking or online purchases, there is no way for both parties to the transaction to verify the outcome. In an internet voting scenario, the only way to verify how someone has voted after the fact is to abandon the secret ballot, which is a non-starter for many reasons.

Canada is not unique in noting these challenges with security, integrity and verifiability in online voting - there are also a number of significant US and other international examples where such weaknesses have been identified. One such example is in Kenya where the highest court overturned a national election due to allegations of voter fraud in the online election.[13] Another example is with the platform Voatz, which was found by MIT researchers in a 2019 paper to have serious flaws, despite using much-vaunted blockchain technology. Voatz has been used in elections in Utah, Oregon, Washington and West Virginia. In their paper, the researchers found that security vulnerabilities would allow a hacker to change a person's vote, stop their vote from being registered, and also identify voters and how they voted.[14]

Another even more recent example came to light through work by Michael Specter of MIT and Dr. Alex Halderman into a company called Democracy Live's OmniBallot platform.[15] As of the date of publication of their paper (June 7, 2020) three US states (Delaware, West Virginia, and New Jersey) had planned to allow certain voters to cast votes online using OmniBallot, despite the established risks of internet voting, and even though the system had never been the subject of a public, independent security review. Regarding the online voting option, the researchers concluded that it "… represents a severe danger to election integrity and voter privacy. At worst, attackers could change election outcomes without detection, and even if there was no attack, officials would have no way to prove that the results were accurate. No available technology can adequately mitigate these risks."[16]

Many such studies examine specific internet voting applications, however it must also be noted that independent bodies with substantial expertise in internet security and privacy have also been tasked with assessing internet voting risks. The US National Academies of Sciences, Engineering and Medicine jointly produced an exhaustive consensus report in 2018 regarding the use of technology in elections called *Securing the Vote: Protecting American Democracy*. The report concluded as follows:

> *At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.*[17]

---

[13] https://www.cbc.ca/news/world/kenya-election-overturned-court-1.4271385
[14] http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 Regarding blockchain: "We further find that their network protocol can leak details of the user's vote, and, surprisingly, that that the system's use of the blockchain is unlikely to protect against server-side attacks."
[15] https://internetpolicy.mit.edu/omniballot-advice/
[16] https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf
[17] https://media.carnegie.org/filer_public/34/9d/349d3207-d994-4838-8b79-5f8d88e0e412/nas_report.pdf

Charter Implications

It is worth reflecting on the fact that the right to vote in federal and provincial elections is protected by Section 3 of the Canadian Charter of Rights and Freedoms. While privacy is a protected right under Section 8 of the Charter in terms of the right to be secure against unreasonable search and seizure, it is arguable that the right to vote in Section 3 also has a privacy component. It is doubtful that the right to vote under Section 3 can be said to have been fulfilled if the secrecy of the vote cannot be guaranteed, not to mention if there are challenges with verifying the result of the election or other integrity issues that arise with internet voting.

The Supreme Court of Canada itself has weighed in on the importance of public confidence in the electoral system in *Harper v. Canada (Attorney General)*:

> *103 Maintaining confidence in the electoral process is essential to preserve the integrity of the electoral system which is the cornerstone of Canadian democracy. In R v. Oakes, 1986 CanLII 46 (SCC), [1986] 1 S.C.R. 103, at p. 136, Dickson C.J. concluded that faith in social and political institutions, which enhance the participation of individuals and groups in society, is of central importance in a free and democratic society. If Canadians lack confidence in the electoral system, they will be discouraged from participating in a meaningful way in the electoral process. More importantly, they will lack faith in their elected representatives. Confidence in the electoral process is, therefore, a pressing and substantial objective.*[18]

Much of the discussion around introducing electronic voting has tended to focus on public engagement to determine whether there is sufficient public acceptance of internet voting, for the purpose of assessing the willingness of the electorate to adopt this method. Research for this paper has uncovered very little engagement at the municipal or provincial level in Canada focusing on whether internet voting is in fact a demonstrably secure method of voting, consistent with the secret ballot. In many cases, the rationale behind the introduction of internet voting is simply a good faith intention to make voting more convenient. This has been facilitated by the presence in Canada of a number of enthusiastic vendors of internet voting systems, who are all too willing to make the transition to internet voting as easy as possible. These venders are the same companies whose systems were assessed in the above-noted study of Ontario's most recent municipal election.

Increasing voter turnout is often cited as a reason to pursue internet voting. In the 2016 Report of the Parliamentary Special Committee on Electoral Reform[19] there was testimony from Nicole Goodman, Director of the Centre for e-Democracy[20] and Assistant Professor at the Munk School of Global Affairs, that Ontario municipal elections using internet voting saw increased turnout of approximately 3%. That figure refers to the 2014 Ontario Municipal Election voter turnout statistics, in which the turnout was

---

[18] Harper v. Canada (Attorney General), [2004] 1 SCR 827, 2004 SCC 33 (CanLII) http://canlii.ca/t/1h2c9
[19] https://www.ourcommons.ca/DocumentViewer/en/42-1/ERRE/report-3/page-291#87

[20] The Centre for e-Democracy, which is often cited in news articles about online voting, was co-founded in 2014 by the CEO of Delvinia. Delvinia currently describes itself as a global research company, but it has also been engaged in the promotion of internet voting, particularly in the City of Markham municipal elections in 2003, 2006 and 2010. Delvinia's web site describes the Centre for e-Democracy as "industry-led": http://www.delvinia.com/centre-for-e-democracy/

43%. The statistics indicate that voter turnout in the 2018 election (which also used internet voting) declined to 38.29%.[21] The Association of Municipalities in Ontario indicates that the lowest voter turnouts on record prior to this were in 1997 and 2003 when turnout was 40%.[22] Given that there has been an increase in Ontario municipalities using internet voting in recent years, the experience there cannot be cited as evidence that internet voting has had or will have a positive impact on voter turnout. It was also noted in the 2016 Parliamentary Report on Electoral Reform that, despite assumptions to the contrary, online voting has no discernable impact in terms of encouraging youth to vote. Seniors, who are already the largest voting bloc, were the most likely to use internet voting.

Even if, despite the lack of evidence, it were to be accepted for the sake of argument that a small increase in voter turnout can be sustained over the long term with the introduction of internet voting, how does that presumed benefit stack up against the vulnerabilities and risks inherent in online voting? If we proceed on the basis that a secure electoral process that guarantees a secret ballot may in fact be a Charter right, a useful framework to assess this question would be the Oakes test.

In summary, the Oakes test is one that has been established by the Supreme Court of Canada to assess actions or measures that impact a Charter right, to allow the Court to determine whether the level of impact is permissible, or on the contrary, whether it has been found to violate the Charter and must be prohibited or struck down.

In assessing a given measure, whether it is the introduction of electronic voting or any other measure, the questions to be asked are:

i. Is the measure demonstrably necessary to meet a specific need?
ii. Is it likely to be effective in meeting that need?
iii. Is the impact on a Charter right (in this case, both the right to vote and the right to privacy) proportional to the need?
iv. Is there a way to meet the identified need without impacting a Charter right, or by impacting it to a lesser degree than the measure as proposed?

The Oakes test starts with the identification of a particular measure that is demonstrably necessary to meet a specific need. It should be noted that not every government policy initiative is driven by a need or problem that must be addressed. Often what is assumed to be a policy problem may in fact be a perceived service expectation. With so many other services available online such as drivers' licenses, banking, shopping, etc., people may expect that all services can be provided online, and perceptions about those expectations may filter up to governments who seek to fulfil public expectations. But an expectation or desire on the part of the public is not necessarily a public policy problem that needs to be solved, or one that can be presumed to pass muster from a Charter perspective, aside from any other risks.

It will be left to legal scholars and the courts to determine the finer points of this issue, including whether municipal elections even attract the same Charter protection as provincial or federal elections, however even if there were no Charter issues at stake, the Oakes test makes for a useful policy analysis framework.

[21] https://elections.amo.on.ca/web/en/home
[22] https://elections.amo.on.ca/web/en/stats

From a policy analysis perspective, the useful questions can be framed as follows:

1) what is the problem to be addressed?
2) what are the causes of the problem?
3) what are some potential solutions?
4) are the solutions likely to be effective?
5) will the potential solutions cause other problems and are those other problems worse than the initial problem?

In reviewing reports and public documentation from Canadian jurisdictions where internet voting has been implemented it appears that there has been little to no concerted effort on the part of governments, prior to implementing internet voting, to 1) identify the problem to be addressed and 2) understand what has caused the problem.

In the case of internet voting, it is not even clear that there is a problem. If the problem can be framed as lack of participation in the democratic process, this is a much broader problem than the method of voting. If the intention is to simply increase the numbers of voters, it is clear from the evidence that internet voting as a solution does not hold water. In addition to the statistics from Ontario municipal elections noted above, BC's Panel on Internet Voting, which recommended that the paper ballot be retained, determined that the evidence for any impact on voter turnout from internet voting is mixed at best. The Panel concluded that the primary purpose of internet voting is as a convenience for people who had already intended to vote. If the problem to be addressed is in fact the broader one posited of a lack of participation in the democratic process, we may be able to skip all the way to number 4 for an easy answer, which is that internet voting is not likely to be an effective solution.

Furthermore, it is also clear from the available research that internet voting carries a number of substantial risks, not only to privacy, but also to the integrity of the electoral process, which could ultimately lead to a lack of confidence in the system itself. These problems arguably outweigh the hoped-for outcome from internet voting of higher voter turnout, particularly given that the evidence for such an outcome is mixed and the risks of harm to the integrity of the electoral system are well established.

Anyone tasked with assessing this issue may wish to consider starting with questions 1 and 2 before even considering a range of potential solutions beginning at question number 3. Even if it were to be determined, after assessing the problems facing our democracy and the causes of those problems, that internet voting should be considered as a potential solution, it should be no more than one of a number of potential solutions to be considered. Furthermore, all of those solutions should be assessed in light of questions number 4 and 5 – which solutions will actually be effective in addressing the problem, and finally, could one or more chosen solutions actually cause other, greater problems? Included in this final assessment, given the Charter rights that are inherent in the act of voting, must be an assessment to ensure that any such solutions will not violate the Charter.

Internet Voting and *ATIPPA, 2015*

Let us assume for the sake of argument that a decision has been made to proceed and that internet voting is indeed a publicly supported initiative that can address a legitimate social need. There is one further consideration. As noted above, *ATIPPA, 2015* applies to any collection, use or disclosure of

personal information by a public body, including both the Office of the Chief Electoral Officer for provincial elections and all municipalities.

One of the most important provisions of *ATIPPA, 2015* is the requirement in section 64 that heads of public bodies take steps that are "reasonable in the circumstances" to keep personal information secure. As noted by the Supreme Court of Canada in *Harper v. Canada (Attorney General)*, "confidence in the electoral process is, therefore, a pressing and substantial objective." It can be argued, therefore, that meeting the *ATIPPA, 2015* threshold which requires that security must be "reasonable in the circumstances" when it comes to personal information collected, used or disclosed in the electoral process, that threshold will be on the higher end of the continuum of reasonable security. One of the reasons it would have to be higher than for other kinds of personal information is because of the relevant circumstances, specifically, the fact that the electoral process is foundational to our democratic society and institutions. Because government decisions have a profound impact on individuals, groups and the population as a whole, voting must be held to the highest reasonably achievable security standard.

The other reason is that, unlike other kinds of personal information in which there are reliable ways to check for errors or to detect malign actors, the requirement for a secret ballot makes it impossible to guarantee such a level of security in an electronic context. Through long experience, we know that the systems and processes in place for paper ballot voting meet that standard. It is certainly not possible now, and it is unclear when or if internet voting will ever achieve that standard, due to the unique characteristics of elections which are different from all other forms of activity on the internet.

Voting During a Pandemic

Since the emergence of COVID-19 there may be understandable concerns about how the electoral process can be adapted to ensure that voting is safe for citizens. This may in turn lead to speculation that, despite its risks, perhaps internet voting will become necessary in order to hold elections while COVID-19 persists. Democratic jurisdictions throughout Canada and around the world must find ways to run elections despite the pandemic and to mitigate the associated challenges.

Perhaps the first to do so was South Korea. South Korea held elections for 300 seats in its National Assembly on April 15, 2020 during the height of the pandemic. In a technical paper, international election consultant Antonio Spinelli outlined all of the various adaptations that South Korea's electoral authorities put in place in order to ensure a safe election, such as enhancing early voting opportunities, social distancing at polling stations, personal protective equipment for poll workers, communication with the public so that they were comfortable with these measures and understood what to expect, etc.[23] Although there were fears that voter turnout would be affected, this did not materialize, and in fact the 2020 election experienced a higher than usual voter turnout. Spinelli's paper outlines a number of lessons that can be adapted by other jurisdictions from the experience in South Korea, and no doubt other jurisdictions will build on and refine those over time. At the very least, South Korea's example shows that, even during a pandemic, traditional elections can be successfully run with the right preparation.

[23] https://www.idea.int/sites/default/files/publications/managing-elections-during-pandemic-republic-korea-crucial-test.pdf

Other Considerations

The introduction of internet voting may offer the notion of convenience and the sense that we have moved elections into a more modern era, but even if the privacy and security issues could easily be resolved, there may be other benefits associated with traditional voting that have not been given due consideration. If one of the purposes of internet voting is the hope that it will lead to increased engagement, consider the fact that traditional elections mobilize a significant segment of our population and engage them actively in the electoral process. From poll clerks to scrutineers, a large number of people play an active role in our democracy on election day, whether they work for the electoral authority or they volunteer to drive people to the polls on behalf of candidates. This is all part of the excitement of election day, and all of those people can say that they have played a role in making it happen. At the polling station, neighbours greet each other and renew acquaintance, and in doing so they share the tangible experience of coming together to decide who will govern them.

If the purpose of reviewing our electoral process is to increase political engagement and participation, we might do well to start there. Are people politically disengaged? If so, why? Do people sometimes feel that their vote doesn't matter? Is the electoral system itself part of the issue? Is our form of government failing us? What other ideas might enhance participation and engagement in our democracy? There are many other questions worthy of consideration and ideas to explore.

Conclusion

One may indeed wonder whether anyone would bother to hack a municipal or provincial election in this Province. The Office of the Chief Information Officer, which is responsible for computer systems within government, records thousands upon thousands of attempted hacks, many from the countries that are often identified as the "usual suspects." The world today is experiencing a decline in the number and strength of democratic governments. Social media manipulation of voters is in full swing, and may already have affected electoral outcomes. Electronic electoral infrastructure in the US has already been targeted by hackers. Under the circumstances, it would seem unwise to experiment with this aspect of our democratic process. Even if an election in this province is never successfully hacked and the electronic processes work as intended, will everyone believe it? If a surprise electoral victory occurs, will people say there was a bug in the system or that it was hacked? If an unknown candidate ekes out a surprise victory against a political veteran, will people be suspicious? There are real security risks involved in the introduction of internet voting, but the real casualty may be the loss of trust in democracy itself, which is perhaps the worst possible result.

There is no electronic system which cannot be hacked. There is no electronic system that is guaranteed to be without flaws. Every hack is not detected. Information security experts typically advise that the question around privacy breaches is not "if" but "when." Should we therefore entrust electronic systems with our banking, our health, and other vital information and transactions? Absolutely we should. As long as we continue to assess and upgrade them to the best available security standards, the benefits those systems provide in enhanced service delivery far outweigh the risks. That is because the risks in most transactional processes are mitigated by the fact that there is an opportunity for verifiability at both ends, and furthermore if oversight is required to address disputes, the evidence is available to the courts about what information was available to whom and when.

There may be non-internet forms of electronic voting which could be explored for consideration within the electoral process. A kiosk voting system that allows users to vote on a touch screen but where a

paper ballot is printed which can be viewed and verified by the voter before placing it in the ballot box may be an option. In such a system the paper ballot would remain the official ballot (and is thus available for recount), while the touch screen simply allows for quick tabulation when the polls close. It also eliminates the possibility of spoiled ballots, and in recounts, only the paper ballot is considered, not the electronic record. There are many different vendors of kiosk systems, some of which have been found to have serious flaws, and many of which do not involve use of paper ballots as the official ballot, therefore close scrutiny is required before any such system could be considered.

If, despite all of the risks, there is a determination, either provincially or municipally, to move forward with internet voting, the first step should be a security assessment by computer security experts who have experience in reviewing and assessing internet voting systems. Such analysis should be independent of the internet voting industry and independent of government. This should precede any public engagement or legislative review aimed at moving toward internet voting, because unless the security standard can be assured, other considerations cannot prevail.

Those who have studied the subject of internet voting and consulted widely with internet security experts tend to conclude that internet voting is unwise. Some security experts offer the view that the technology is currently not sufficiently advanced, while others offer the view that it can never match the security, reliability, anonymity and verifiability of paper voting.