Appendix I

Internet and Telephone Voting in Nova Scotia

Background

Public opinion in support of Internet and telephone[1] voting has been growing. Elections Nova Scotia is frequently asked why Nova Scotia electors cannot vote online or by phone in provincial elections when they've been able to do Internet and telephone banking for years. As well, in recent years, a number of municipalities and school boards in the province have used telephone and web-based voting as an option in their elections.

In October 2012, several municipalities, including the Cape Breton and Halifax Regional Municipalities, used Internet and telephone voting.

At the federal level, Elections Canada had announced its intention to pilot Internet voting in a by-election in 2013 but has since backed-off on the date. At the provincial level, Elections Ontario announced a pilot of both Internet and telephone voting in a future provincial by-election, and Elections British Columbia has appointed an independent five-person panel to study Internet voting at the request of the BC Legislature.

With these developments in mind, the chief electoral officer asked the members of the Election Commission of Nova Scotia[2] their opinion regarding the advisability of preparing for Internet and telephone voting during provincial elections. After considering the literature available, including a careful review of Elections BC's Discussion Paper on Internet Voting[3], the Commission members developed a unanimous position that it is premature to entertain either Internet based or telephone voting options at this time.

The Commission members point out that it is the Members of the Legislative Assembly (MLAs) in Nova Scotia who must ultimately decide public policy on permitting the use of Internet or telephone voting in a provincial general or by-election. The convenience and accessibility benefits espoused by the proponents of these forms of electronic voting are tempting to the general public, but in the end the decision will depend heavily on the comfort level MLAs have with answers to five important questions posed below.

In the interest of fostering public education and informed debate, the Election Commission members have laid out their thoughts on the present status of answers to these five essential questions.

1) How secure are Internet and telephone-based voting transactions?

Elections BC points out that banks knew from the beginning that online banking would not be fraud proof. They calculated that the money they would save in reduced operating costs would make up for the money they would lose to online banking fraud. They have insurance to reimburse their clients' financial losses. The problems banks encounter with online banking fraud have been on the increase, which is forcing these institutions to spend substantially more resources on insurance, reimbursements to defrauded customers, and for the development of new security strategies to keep pace with ever-evolving and increasingly sophisticated fraudulent activities.

The outcome of a provincial election affects every citizen in Nova Scotia. Banking transactions, on the other hand, take place between individual clients and their bank; the consequences of a dispute do not directly affect anyone else. The public needs to know that each vote in an election was made by an individual, legitimate, elector; that the secrecy of each ballot was preserved; and that each vote choice recorded was accurately counted exactly as it was cast. The integrity of every election depends on these fundamental components being preserved. The Province's MLAs will need to be satisfied that any service vendor being considered for providing Internet and telephone voting services can demonstrate in advance that their system meets these minimum requirements without question.

2) Can service availability be guaranteed?

If an online or telephone banking service is unavailable, clients can try again at a later time or visit their local branch or any bank or ATM offering Interact. However, elections are delivered according to a legislated calendar that provides extremely limited flexibility. For example, if election day is October 9th, voting cannot be extended under any circumstances to October 10th.

There are several potential reasons that online and telephone voting services

[1] *Telephone voting systems have evolved to making use of Voice Over Internet Protocol (VOIP) technology. As a result, the same infrastructure that collects voting choices via a web page interface can allow telephone devices to simply act as a different interface to the same election application.*

[2] *The Election Commission of Nova Scotia is a seven-member panel made up of appointees from the three registered parties represented in the Assembly with the chair appointed by Order-in-Council. The Commission regularly provides advice to the Chief Electoral Officer and reports back to the registered parties on topics of interest being considered by Elections Nova Scotia in the administration of the provincial electoral process.*

[3] *http://www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf, August 2011*

could lose availability during a critical time period (e.g. denial of service attack, hacking, software bug or hardware malfunction, power or network outage, under-estimated service capacity requirements), and this could mean that electors would lose their chance to vote or even have their vote invalidated.

In the recent municipal elections in Nova Scotia, both Cape Breton Regional Municipality and Halifax Regional Municipality used Internet voting exclusively for advance poll voting, but not on election day. This mitigated the lack of service risk factor by offering electors a final opportunity to vote in the traditional way on election day.

If all other concerns were adequately addressed, MLAs might consider the initial use of Internet or telephone voting as one of several options available within an election but start with making the electronic voting channels accessible only during periods outside of election day.

3) How do you know it is me voting?

Banking transactions are identifiable with a complete audit trail from end to end. The client has an established relationship with the bank, transactions require user authentication through user IDs (unique identification codes) and PINs (unique personal identification numbers), and the client's identity follows the transaction through to its completion.

Democratic voting is different. How a person votes is guaranteed to be private and this fundamental democratic principle of ballot secrecy requires that there is no linkage possible between a ballot and the identity of the person who used it. In an election, an elector's identity is authenticated only to confirm eligibility.

With the exception of the limited use of a mail-in write-in ballot option (used primarily by military electors and out-of-province electors), the current provincial voting procedures ensure a person's privacy by requiring them to vote in person by themselves behind a privacy screen in a supervised environment. That privacy ensures electors cannot be coerced into a voting choice, their vote cannot be bought, and they will not experience any repercussions because of their choice.

Some might argue that secrecy is compromised and coercion is possible when immediate family members accompany an elector when voting. Except for someone acting as a 'friend' to a voter who requests assistance in marking their ballot, and has taken the required secrecy declaration, or a young child of the voter who is permitted for educational purposes, no one is allowed to accompany a voter behind the privacy screen in a traditional provincial polling station.

Experts warn that currently no transaction using the Internet can be guaranteed to be secure. Despite advances in security, there is still the chance a voter's identity and voting choice could be exposed, or that someone could vote with someone else's credentials.

The possibility of collecting family members' PINs and then voting on their behalf increases significantly in the privacy of one's own home. At their very best, lists of electors rarely surpass a 95 percent coverage and accuracy level. Under Internet or telephone voting arrangements, the chance of being caught voting on behalf of someone else is minimal. This could potentially happen through the use of voter information cards and PINs of recently deceased family members, or former residents of a particular address, or simply by voting for an absent family member with or without their consent.

There is also the possibility of organized fraudulent activities such as collecting Voter Information Cards and mailed PINs left in the lobbies of apartments, condominiums, and student or seniors' residences. Access to information such as electors' birth dates would be difficult, but not an insurmountable obstacle, given the extensive data collected by various private and public entities and the amount of information posted on the Internet. Someone who had access to such data, by whatever means, could vote in volume from a high traffic VPN or telephone system network cluster, and detection would be extremely difficult.

None of the above-described actions would be legal if Internet or telephone voting was used,but all would be difficult to detect. Given that the average number of electors per electoral district in Nova Scotia is about 14,000, even a limited uptake of any of these examples of illegal voting could affect the outcome of a close election.

To the members of the Election Commission, a satisfactory response to this problem of reliable authentication must precede the adoption of any widely-used form of Internet and telephone voting.

4) Is there an audit trail I can follow?

In banking, an audit trail shows exactly how monies are allocated. If fraud is suspected, it can be readily identified through a review of the records because the "before state" (or amount of money originally in the account) is known and provable with documented records. Clients can detect errors themselves by reviewing their regular statements.

In the existing traditional paper based voting system, questionable results can be resolved in a similar manner. A record exists of how many people voted and identity information (but not how they voted) exists about each person who cast a ballot at an assigned ballot box. That is the "before state." Ballots can then be physically verified and recounted by a provincial court judge. The number of ballots counted must correspond exactly to the recorded number of people who voted at that polling station.

Perhaps the largest leap of faith with Internet and telephone voting is the fact that there is no "before state" examinable. While an auditor can easily demonstrate that the number of votes cast equals the number of votes counted, there remains considerable debate whether there is a satisfactory and transparent way to compare how many of those votes were actually cast by electors verified as registered and not having voted before, and whether each vote was accurately recorded by the software used.

Provincial legislation requires an automatic judicial recount if the difference between the first and second candidate is six votes or fewer. Where paperless votes were cast, how would a judge review each of the votes cast? Would that judge need to be, or have the assistance of, a forensic computer technician to make an accurate determination?

In Germany a court ruling has declared electronic voting unconstitutional because people without technical expertise and specialized knowledge are unable to scrutinize the process.

5) Can I watch the count?

Banks are private entities and are allowed to use secret processes to protect their online transactions. Secret security processes, however, are not acceptable measures for those aspects of electoral democracy where credibility is directly tied to transparency.

The traditional method of voting achieves transparency by having the acts of voting and counting take place in controlled physical locations, where observers representing all interested parties can witness the process and ensure that all required procedures are properly followed.

Technology encases the voting and counting process in a "black box," which reduces transparency and, potentially, public confidence. This can be addressed if the actual software used in Internet or telephone voting is open to public scrutiny by independent and trusted programmers and technical analysts before, during, and after the electoral event. It is our understanding that none of the companies currently offering Internet and telephone voting services are willing to share their proprietary software with the public. While this is understandable for both commercial and security reasons, it is problematic in terms of meeting the widely-accepted democratic principle of procedural transparency in ballot issuance and vote counting procedures.

In addition to the known insecurities, a provincial general election conducted on an Internet platform for web or telephone voting could elicit new levels of unknown threats from hackers seeking to gain a high profile from a successful attack. Consider also that the most serious attacks would likely come from persons or groups motivated to change the outcome without anyone noticing.

With that in mind, the adversaries of an election system would not likely be amateurs in basements but interested groups and individuals with a significant stake in the outcome of an election.

Conclusion

Those in favour of Internet and telephone voting argue that they provide such improved levels of accessibility that they can increase voter turnout and reach people who would not vote if required to attend a physical voting site. By the very nature of services being offered, improved access to voting for many electors is an acknowledged benefit. Even with the recent successes observed in the municipal elections in Nova Scotia in fall 2012, where a significant percentage of electors voted by phone or on the web, some saw increased voter turnout, but this was not the experience for all municipalities. And, while most would agree that online voting is consistent with our increasingly online society, the basic questions of how to maintain the security, validity, and integrity of our elections has not yet, in our opinion, been satisfactorily answered.

Until credible answers to these questions are available, and until functioning, transparent Internet and telephone voting systems have been demonstrated and proven, extreme caution and prudence is required.

Michael Coyle, *Chair*
Susan E. Hayes, *Representative Nova Scotia Liberal Party*
Chris MacInnes,*Representative Nova Scotia Liberal Party*
Susan Dodd,*Representative Nova Scotia New Democratic Party*
Don Fraser, *Representative Nova Scotia New Democratic Party*
Jeff Hunt, *Representative Progressive Conservative Association of Nova Scotia*
Cameron MacKeen, *Representative Progressive Conservative Association of Nova Scotia*