Independent Panel on

Internet Voting

BRITISH COLUMBIA

Recommendations Report to the Legislative Assembly of British Columbia

February 2014

Independent Panel on
Internet Voting
BRITISH COLUMBIA

PO Box 9275 Stn Prov Govt, Victoria, BC, V8W 9J6
Enquiries: 250-387-5305 or Toll-free at 1-800-661-8683
Email: info@internetvotingpanel.ca
Website: internetvotingpanel.ca

February 12, 2014

Honourable Linda Reid
Speaker of the Legislative Assembly
Room 207
Parliament Buildings
Victoria, B.C. V8V 1X4

Dear Madame Speaker:

I have the honour to submit the Recommendations Report to the Legislative Assembly of British Columbia – February 2014.

This report is filed in accordance with section 13(1)(d) of the *Election Act*.

Respectfully submitted,

Keith Archer, Ph.D.
Chief Electoral Officer
British Columbia
Chair, Independent Panel on Internet Voting

Independent Panel on
Internet Voting
BRITISH COLUMBIA

PO Box 9275 Stn Prov Govt, Victoria, BC, V8W 9J6
Enquiries: 250-387-5305 or Toll-free at 1-800-661-8683
Email: info@internetvotingpanel.ca
Website: internetvotingpanel.ca

February 12, 2014

Members of the Legislative Assembly of British Columbia,

Beginning in September 2012, the members of the Independent Panel on Internet Voting reviewed best practices with respect to Internet voting in other jurisdictions and examined issues associated with implementing Internet voting for provincial or local government elections in British Columbia.

A Preliminary Report was made available on the panel's website (internetvotingpanel.ca) for a six-week public comment period from October 23 to December 4, 2013. The panel reviewed the commentary on Internet voting and the Preliminary Report, including additional submissions from experts, academics and vendors in the Internet voting community.

The following *Recommendations Report to the Legislative Assembly of British Columbia – February 2014* expresses the panel's conclusions and recommendations. In developing the report, the panel focused much of its effort on evaluating the benefits and challenges of implementing Internet voting in British Columbia. The report includes a summary of the panel's assessment of those benefits and challenges and a summary of lessons learned from other jurisdictions.

The report also contains a number of appendices, a list of references, and case studies of the experiences with Internet voting in other jurisdictions. A complete bibliography of the materials reviewed and considered is included on the panel's website.

The panel thanks everyone who participated in the public process and for taking the time and effort to engage in the important discussion. All panel members concur with the conclusions and recommendations detailed in this report.

Dr. Keith Archer, Chair

Dr. Konstantin Beznosov

Lee-Ann Crane

Dr. Valerie King

George Morfitt, FCA

CONTENTS

1.0 EXECUTIVE SUMMARY

The Independent Panel on Internet Voting (the panel) was formed by the Chief Electoral Officer on August 9, 2012, following an invitation of the B.C. Attorney General, to examine opportunities and challenges related to the potential implementation of Internet-based voting as a channel of voting for provincial or local government elections in British Columbia. The panel, comprised of the Chief Electoral Officer and four additional members, met 13 times between September 2012 and October 2013. In that time the panel reviewed the existing and evolving literature and spoke to a variety of experts in the fields of technology, Internet security and electoral administration. The panel examined research on both the benefits of and challenges to implementing Internet voting and heard from experts strongly in favour of and strongly opposed to the idea of implementing Internet voting in British Columbia.

A report outlining the panel's preliminary conclusions and recommendations was made available for public comment between October 23, 2013 and December 4, 2013. The panel heard from over 100 individuals and from experts in the field of Internet security, vendors of Internet voting technologies, and groups representing persons with disabilities. At the conclusion of the public input period, the panel met an additional two times to consider the input and produce this report. The public input largely reaffirmed the panel's thinking as expressed in the preliminary report.

This report is intended to provide the Legislative Assembly with a review and assessment of the prospects for Internet voting in British Columbia. It is intended that Members of the Legislative Assembly will use this report to become informed regarding the concepts, principles and arguments made both for and against implementing Internet voting at either the local or provincial government level.

1.1 Conclusions and recommendations

The panel concludes that Internet voting has the potential to provide some benefits for administering local government elections and provincial elections in British Columbia and that the most significant potential benefit of Internet voting is increased accessibility and convenience for B.C. voters. Other presumed benefits, such as increased turnout and lower cost are not typically realized.[1]

The panel also concludes that Internet voting has some significant inherent risks. It is important to understand that although the Internet is used for an increasing number of interactions (such as banking, shopping, dating, planning trips, and the like) with their own risks, voting over the Internet has a set of unique challenges that inevitably introduce a number of additional risks. The extent to which each of these risks can be mitigated or eliminated also depends on the details of the way in which an Internet voting model is implemented. Security at the voter's device,[2] reduced transparency and

1 For more on the potential benefits of implementing Internet voting, see 4.0 Perceived and actual benefits of Internet voting, page 12

2 References in this report to the voter's "device" can be read as any means by which an individual could cast a ballot for Internet voting (e.g., computer, tablet, smartphone)

auditability compared to traditional voting methods, and cost were seen by the panel to be the most significant challenges to implementing Internet voting for either local government or provincial government elections.[3]

While Internet voting has been investigated by various jurisdictions around the world over the past fifteen years, it is still not widely implemented. Internet voting is used in only a limited number of jurisdictions, and only on a limited basis.

Weighing the benefits and challenges to implementing Internet voting in specific circumstances is the role of policy-makers. There is a high level of trust in the current voting processes used at the local and provincial government levels, but there are opportunities for improvement in each. The panel believes that Internet voting has the potential to be an additional voting channel for voters with specific accessibility challenges in future local or provincial government elections, provided that the recommendations outlined in this report are followed and any system implemented complies with the principles established by the panel. The panel believes it is not feasible for this to occur in time for the 2014 local government elections.

To guide members of the Legislative Assembly, and potentially local government officials, in their task of weighing the benefits and risks of Internet voting, the panel sets forth the following recommendations:

1. **Do not implement universal Internet voting for either local government or provincial government elections at this time. However if Internet voting is implemented, it should be limited to those voters with specific accessibility challenges. If Internet voting is implemented on a limited basis, jurisdictions need to recognize that the risks to the accuracy of the voting results remain substantial.**

   The risks of implementing Internet voting in British Columbia outweigh the benefits at this time. Therefore it is premature to implement Internet voting on a universal basis.

   Because of the strengths of Internet voting to provide increased accessibility for certain segments of the population (e.g., remote voters, voters with disabilities and voters who would otherwise need assistance to vote), Internet voting could be used in the future on a limited basis to improve access to the ballot for these groups. There are significant risks to implementing Internet voting that can jeopardize the integrity of an election, no matter the extent of implementation. If Internet voting is to be used in British Columbia in the future, the following three recommendations must be adhered to, including all of the principles outlined in recommendation #4.

3 For more on the challenges to implementing Internet voting, see 5.0 Perceived and actual challenges to implementing Internet voting, page 22

2. **Take a province-wide coordinated approach to Internet voting.**

   If Internet voting is to be implemented at either the local government or provincial government level, election administrators should work with each other and with the provincial government to conduct a more rigorous review of the options, establish a common framework for implementation and retain control and oversight over election administration during implementation.

3. **Establish an independent technical committee to evaluate Internet voting systems and support jurisdictions that wish to implement approved systems.**

   Provincial and local government election administrators do not have the necessary technical expertise in-house to properly evaluate, verify and test high security systems such as Internet voting systems. A technical committee independent from vendors, political parties, and elected representatives, and made up of election administrators and recognized experts in Internet voting, cryptography, and computer security should be established to support the province-wide coordinated approach. The technical committee would be established by, and would report to, the B.C. Chief Electoral Officer. Such a reporting structure would emphasize the technical committee's independence. Such a committee would have to stay abreast of changes in available and emerging technology in order to establish standards and requirements that would have to be met by any Internet voting system to be used in British Columbia. The committee would also be responsible for overseeing a rigorous review of any system being considered for use against those standards and requirements to ensure high security. Only Internet voting systems approved by the technical committee should be authorized for use in B.C. jurisdictions. The technical committee would also be responsible for monitoring the security of the systems while in use and conducting a full audit and evaluation afterwards. The work of the technical committee should be made public to ensure transparency and to build trust in any system implemented.

4. Evaluate any Internet voting system against the principles established by the panel.

While acknowledging that there will be unique factors to consider in each jurisdiction, the panel recognizes the benefit of establishing a common, or at least similar, set of principles that can be used by multiple jurisdictions in Canada to evaluate Internet voting. There is a growing consensus among election administrators of what these principles are. The panel used the eight principles established by Elections Ontario in its Alternative Voting Technologies Report[4] as a starting point from which to develop principles for British Columbia. Many of the principles outlined below share common elements with Elections Ontario's principles, but some have been amended to reflect a B.C. context or for consistency with the language used in this report. These principles must be met in addition to any standards a technical committee would establish.

Accessibility

The Internet voting process must be readily available to, and usable by, all voters eligible to vote by Internet voting, even in the presence of Internet voting-specific threats.

Ballot anonymity

The voting process must prevent at any stage of the election the ability to connect a voter and the ballot(s) cast by the voter.

Individual and independent verifiability

The voting process will provide for the voter to verify that their vote has been counted as cast, and for the tally to be verified by the election administration, political parties and candidate representatives.

Non-reliance on trustworthiness of the voter's device(s)

The security of the Internet voting system and the secrecy of the ballot should not depend on the trustworthiness of the voter's device(s).

One vote per voter

Only one vote per voter is counted for obtaining the election results. This will be fulfilled even in the case where the voter is allowed to cast their vote on multiple occasions (in some systems, people can cast their vote multiple times, with only the last one being counted).

4 Reference #292

Only count votes from eligible voters

The electoral process shall ensure that the votes used in the counting process are the ones cast by eligible voters.

Process validation and transparency

The procedures, technology, source code, design and implementation details, and documentation of the system must be available in their entirety for free and unconstrained evaluation by anyone for testing and review for an appropriate length of time before, during and after the system is to be used. Policies and procedures must be in place to respond to issues that arise. Appropriate oversight and transparency are key to ensuring the integrity of the voting process and facilitating stakeholder trust.

Service availability

The election process and any of its critical components (e.g., voters list information, cast votes, voting channel, etc.) will be available as required to voters, election administrators, observers or any others involved in the process. If Internet voting should become unavailable or compromised, alternative voting opportunities should be available.

Voter authentication and authorization

The electoral process will ensure that before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, and that the voter is eligible to vote

2.0 INTRODUCTION

2.1 The Independent Panel on Internet Voting

Three key developments led to the forming of the Independent Panel on Internet Voting:

- March 2011 – The City of Vancouver requested approval from the Minister of Community, Sport and Cultural Development to use Internet voting for the November 2011 local government elections. The request was not granted and the 2011 Local Government Elections were held in the traditional manner.
- August 2011 – Elections BC submitted *Discussion Paper: Internet Voting* to the Legislative Assembly to further public dialogue on the topic.
- November 2011 – The Chief Electoral Officer submitted to the Legislative Assembly the Report of the Chief Electoral Officer on Recommendations for Legislative Change. Of the four recommendations in the report, one was entitled Trialing New Voting Technologies and suggested that "legislators may wish to consider providing greater flexibility to the Chief Electoral Officer to introduce, on a pilot basis, a variety of new voting technologies." This recommendation was intended to cover a host of technologies including, but not limited to, Internet voting and to increase the possibilities for further detailed assessment of new voting technologies in British Columbia.

On August 7, 2012, the Minister of Justice and Attorney General invited the Chief Electoral Officer to convene a non-partisan panel to review best practices with respect to Internet voting in other jurisdictions and to examine the issues associated with implementing Internet voting in British Columbia. The request included that the panel examine Internet voting in both local and provincial contexts.

On August 9, 2012, the Chief Electoral Officer responded to the Minister of Justice and Attorney General advising that he was pleased to convene and chair such an independent panel and laid out how he would proceed in doing so.

> Authority: convening a panel to research and draft recommendations to the Legislative Assembly is authorized pursuant to section 12(2)(a) of the *Election Act*
>
> Scope: building upon the *Discussion Paper: Internet Voting*, the panel will examine opportunities and challenges related to the potential implementation of Internet-based voting for provincial or local government elections in B.C.
>
> Reporting: the method for gathering input and feedback from experts and the public will be determined by the panel, as will a timeline for reporting

Composition: the Chief Electoral Officer will chair the panel and invite four additional members; members will be drawn from a wide spectrum reflecting expertise in technology, cryptography, Internet security policy, and electoral administration; all members will have a high level of independence and judgment

Secretariat: will be provided by Elections BC

Budget: estimated to be $420,000

2.2 The work of the panel

Upon agreeing to convene and chair the panel, the Chief Electoral Officer proceeded to identify and select panellists who had the required expertise, independence and judgement. On September 10, 2012, the composition of the panel was publicly announced.

Panellists were selected based on their expertise and experience, with an eye to ensuring appropriate gender and geographical distribution. All panellists live and work in B.C. Two are university professors with experience in computer science, computer engineering and computer and network security. One is a local government administrator with experience in elections, and one is a former Auditor General.[5]

The panellists agreed early on that they would undertake to educate themselves about Internet voting so as to be able to make informed recommendations to the Legislative Assembly. On that basis, it was decided that the time line for the panel's work would depend largely on what it learned during the examination period. At the same time, the panellists were aware that local governments were hopeful they would learn the recommendations of the panel in sufficient time to plan for the 2014 local government elections under either outcome.

The panel agreed with the Chief Electoral Officer's response to the Minister of Justice and Attorney General that it would use the Elections BC *Discussion Paper: Internet Voting* as a starting point for determining the scope of its work. The panel wanted to build upon the Discussion Paper and learn more about the benefits and challenges to implementing Internet voting and, as well, learn about the jurisdictions that have investigated and implemented Internet voting, both in Canada and around the world.

At its meetings the panel reviewed some of the academic and practitioner literature on Internet voting, received presentations from experts on a variety of topics and reviewed the actual and perceived benefits and challenges to the implementation of Internet voting. The panel divided its time between reviewing material, listening to presentations, and debating the issues that had been identified.

5 For more information about the panellists, see Appendix B – Panel members, page 54

The panel met monthly between September 2012 and February 2013 before a three month hiatus while the Chief Electoral Officer focused his attention on administering the 2013 Provincial Enumeration and Provincial General Election under the existing election administration model. Prior to taking this break the panel determined that it had gathered much of what it had hoped to learn and that, upon resuming its work after the election, it would conclude its information gathering phase, begin its deliberations, and proceed to produce a preliminary report by the fall with preliminary recommendations for public distribution and feedback.

The preliminary report provided the public with a research summary of both the benefits and challenges to implementing Internet voting for provincial or local government elections in British Columbia, and outlined the panel's preliminary conclusions and recommendations. The preliminary report was available on the panel's website (internetvotingpanel.ca) beginning on October 23, 2013 and the panel invited public comment from B.C. residents. Input could be submitted to the panel by the panel website, email address and traditional mail for a six week period concluding December 4, 2013.

During that period the panel received input from over 100 individuals from across British Columbia. Of the comments in favour of Internet voting, common themes included: the potential for increased convenience and the removal of barriers for people with accessibility challenges; the need for voting to keep up with an increasingly digital lifestyle; and anecdotal evidence that Internet voting would lead to increased voter turnout. Of the comments opposed to Internet voting, common themes included: concerns about Internet security generally and the potential for compromised election results because of security challenges; a lack of trust in results that aren't scrutinized in the traditional manner; and a feeling that if Internet voting won't improve voter turnout, it is not worth the risk.

In addition to comments from B.C. residents, the panel also received input from experts in the field of Internet security outside of B.C, as well as from vendors of Internet voting technologies, and groups representing persons with disabilities in B.C.

It cost approximately $150,000 to administer the Independent Panel on Internet Voting.

2.3 Voting in local and provincial government elections

Given the mandate to examine the suitability of Internet voting for both local and provincial government elections, early in the life of the panel the members sought to develop a clear understanding of the existing voting processes used in British Columbia. The panel invited staff of Elections BC and the Ministry of Community, Sport and Cultural Development to brief it on the universal standards for democratic elections and explain to it how they are met in legislation and in practice.[6] The staff also informed the panel about the voting model used at each level of government and the various voting opportunities currently in place. Ministry staff emphasized to the panel that each local government was responsible for the administration of elections in its jurisdiction and, as such, the elections are not administered precisely the same way in each. The following table summarizes the information contained in those presentations:

	Local government elections	Provincial elections
Frequency	Every 3 years (general elections); As required (by-elections, other voting)	Every 4 years (general elections); As required (by-elections, referenda)
Elected offices	▪ Municipal (mayor, councillors) ▪ Regional District (electoral area directors) ▪ Parks boards ▪ School boards (trustees) ▪ Islands Trust	▪ Legislative Assembly (Members of the Legislative Assembly)
Number of positions filled	~1,650 individuals to ~250 government bodies	85 individuals to 1 government body
Administered by	~190 local governments (Chief Election Officer appointed by council or board)	Elections BC (Chief Electoral Officer appointed by Legislative Assembly)
Budget set by	Local governments	Elections BC
Funded by	Local governments	Province
Legislative framework (primary)	*Local Government Act, Vancouver Charter*	*Election Act, Referendum Act*
Legislation covers	Election administration Candidate nominations Conduct of voting Conduct of counting Campaign finance rules Election offences Invalid election procedures	
Voters list used	Subset of provincial voters list; OR Own voters list; OR No voters list (election day registration only)	Provincial list of registered voters, updated on a continuous basis from various sources

6 References #283, 284, 285

Voter registration by telephone or Internet	No	Yes
Voter registration on voting day	Yes	
General Voting Day	Consistent across province	
Advance voting	1 day (consistent across province); 1 additional day for communities over 5000 (day and time set by local government); Additional days at discretion of local government	4 days (consistent across province)
Vote by mail	At discretion of local government	Required
Other voting opportunities	At discretion of local government (special voting opportunities in hospitals, long-term care facilities, or other places where an elector's mobility may be impaired)	At the district electoral office; At any other provincial voting opportunity in the province
Vote by telephone or Internet	No	
Qualifications to vote	Resident elector: ▪ Canadian citizen ▪ 18 years of age or older ▪ Resident of the jurisdiction where you intend to vote for at least 30 days ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting **OR** Non-resident property elector: ▪ Canadian citizen ▪ 18 years of age or older ▪ Have owned property in the jurisdiction where you intend to vote for at least 30 days ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting	▪ Canadian citizen ▪ 18 years of age or older ▪ Resident of the electoral district ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting
Frequency of by-elections	Varies (e.g. 19 by-elections in 2012)	Varies (e.g. two by-elections in 2012)
Frequency of other voting	Varies	Varies (referendum held in conjunction with general elections in 2005 and 2009, stand-alone mail-based referendum in 2011)

3.0 INTERNET VOTING: DEFINITION AND SCOPE

Internet voting refers to a voting method "where votes are transferred via the Internet to a central counting server".[7]

Internet voting can be further separated into on-site Internet voting and remote Internet voting. On-site Internet voting is conducted at controlled settings such as voting places or kiosks established in high-traffic areas where election officials may be available to authenticate voters and ensure the integrity of the device and software used by voters to vote in private. Remote Internet voting allows voters to cast their ballot from any Internet connection to which they have access, such as a home computer or smartphone.

The Independent Panel on Internet Voting limited the scope of its work to remote Internet voting. Accordingly, both on-site Internet voting and the use of electronic voting and counting machines in the voting place were out of scope.

Internet voting conducted on supervised machines in the voting place could be considered to be a step towards familiarizing voters and election administrators with processes and technology for eventual remote Internet voting. However, on-site Internet voting in the voting place would not provide any accessibility or convenience benefits for voters who would still need to attend the voting place, and does not address many of the security concerns related to Internet voting.

Throughout this report, references to Internet voting should be read as *remote* Internet voting unless otherwise specified.

While Internet voting can, and is, used for some non-governmental elections such as for student groups, trade unions and professional organizations, references to Internet voting in this report are limited to its use in governmental elections.

The purpose of the panel was not to evaluate a particular technology or process for use in B.C. The implementation of Internet voting differs from one jurisdiction to the next. Whether due to differences in public policy, legislation, existing voting processes or the technology chosen by the jurisdiction, there is no common practice for what Internet voting looks like when implemented. Therefore the panel chose to consider many of the ways Internet voting has been implemented to determine if Internet voting in some form could be appropriate for use in British Columbia.

7 Reference #130

4.0 PERCEIVED AND ACTUAL BENEFITS OF INTERNET VOTING

A significant amount of research has been conducted into the benefits of Internet voting, but the research community and stakeholders do not agree on a common list of benefits or a ranking of their relative importance.

In a particular jurisdiction an issue may or may not be a benefit, and could even be seen as a challenge, depending on the perspective of the stakeholder and the specific implementation of Internet voting being considered. Across jurisdictions there is even more disagreement as to whether a perceived benefit of Internet voting can be realized in practice.

The panel chose to examine all of the perceived benefits mentioned in the literature and evaluate for itself what actual benefits could be realized in B.C. by implementing Internet voting for either local or provincial government elections.

4.1 Increase voter turnout[8]

Academic publications suggest that, since the 1970s, citizens in Western democracies have been taking up the act of voting at later points in their life and in smaller numbers, and accordingly overall voter turnout has dropped from approximately three-quarters of eligible voters in the 1970s to approximately half of eligible voters today. In the 2013 Provincial General Election overall turnout was 55.3% of eligible voters, but only 29.9% of eligible voters aged 18-24 chose to vote.[9] At the local government level turnout is also trending down, but to an even lower level. In the 2011 B.C. Local Government Elections, voter turnout averaged 29.6%.[10]

Internet voting is seen by some as a potential solution to this trend of declining voter turnout. It is often claimed that individuals who are not motivated to attend a voting opportunity in their community in person would vote online if given the opportunity. However, political science research into jurisdictions that have implemented Internet voting is more sceptical.

While there have been some Internet voting elections where voter turnout has increased, when other factors such as the apparent closeness of the race and interest in particular contests (e.g., a mayoral election without an incumbent) are taken into consideration, research suggests that Internet voting does not generally cause non-voters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have already decided to vote.

8 For more information on this matter, see references #48, 60, 75, 131, 145, 152, 157, 164, 207, 208, 215, 216, 275, 276
9 Reference #336
10 Reference #228

Some proponents argue that the novelty factor provided by Internet voting leads to voters paying increased attention to otherwise lower interest elections, particularly at the local government level. However, research suggests this increased attention may be limited to the first instances of Internet voting before returning to more typical levels.

Researchers have also looked at the demographics of Canadian voters who have used Internet voting and have found that Internet voting is most popular among middle-age voters and least popular among youth and therefore reflects traditional voter turnout demographics. These findings run contrary to the widely expressed belief that Internet voting will lead to increased participation by youth.

Conclusion

The evidence for Internet voting to lead to increased voter turnout in British Columbia elections appears to be at best mixed, and the panel is not convinced that introducing Internet voting in British Columbia will result in increased voter turnout at either the local or provincial government level in the long run.

4.2 Increase accessibility and convenience[11]

The next most popular potential benefit of Internet voting among proponents is its ability to make voting more convenient and increase the accessibility of the electoral process for those who do choose to vote. Unlike increasing turnout among voters, increasing the accessibility of the process is more in line with the perceived or legislated responsibilities of election administrators.

Under the current provincial voting model, voters have many opportunities to vote outside of their assigned voting place near their home. The provincial absentee voting rules allow a voter to cast a ballot at the local office of the District Electoral Officer, at any voting location in the province, or by requesting a ballot be mailed to them (vote by mail). While the multitude of absentee voting provisions address individuals' absence from their community or the province, it still requires a voter to either travel to a voting place in the province or request, receive and mail back a ballot. Mailing ballots back and forth takes time, which places notable constraints on voters in remote areas or foreign countries. In 2013, approximately one-third of voting packages requested were not returned to Elections BC on time, or at all.[12] Beginning in 2013, Elections BC will mail a write-in ballot to voters up to 30 days before Writ Day for a fixed-date general election, but voters must still wait to mark their ballot until after the writ of election is issued and must mail it back so that it is received before the close of voting on general voting day (28 days after the writ of election is issued).

11 For more information on this matter, see references #48, 131, 136, 142, 144, 146, 194, 204
12 Reference #335.

In 2013, voting packages that were sent to international addresses before Writ Day were returned at a rate significantly higher than those that were sent after Writ Day (60% compared to 38%). Local governments that choose to offer vote by mail are limited to a three week window in which the ballot must be requested, mailed to the voter, marked and mailed back so that it is received by the legislated deadline.

Internet voting could enable voters that currently rely on the vote by mail process to have better access to the ballot and provide these voters with greater certainty that their ballot will be received by the election administration before the close of voting.

As there are fewer absentee voting options at the local government level in B.C. and vote by mail is only offered in some communities, an Internet voting option has the potential to benefit these absentee local government voters.

Providing voters with the opportunity to vote without travelling to a voting place can lower both the financial and time cost of voting. For example, the incremental financial cost to a voter casting an Internet ballot is likely to be less than that for an individual voting in person after having taken time off work, travelling to a voting place, and extending the hours required for child care. Similarly, while the act of voting in person typically takes only five minutes[13] after arrival at the voting place, casting a ballot online would likely be faster than the total amount of time spent planning a change to an existing schedule, travelling to a voting place, casting a ballot and returning home.

In many jurisdictions offering internet voting, it has been offered around the clock during the applicable voting period rather than limited to traditional voting hours. This enables voters to choose to vote at the time most convenient for them.

Local government elections are held on the third Saturday in November every three years. In many communities in B.C., the snow and other bad weather common at that time of year can make it difficult for voters to attend in-person to vote. While local governments in B.C. are petitioning the provincial government to move general voting day up to October, introducing Internet voting would lower the risk of voters in these communities being unable to vote due to seasonal inclement weather. As provincial general elections are held in May, this is less of an issue for provincial voters.

Another benefit of Internet voting is that it has the potential to allow voters with disabilities[14] additional opportunities to vote independently using technology they already have access to and are familiar with. Some Internet voting systems can vary the format of the ballot to meet the needs of individual voters with respect to font sizes, languages, etc. While provincial and local government voters in hospitals and long term care facilities are often visited by election officials in person, many voters with special needs outside of these facilities would also benefit from Internet voting.

13 Reference #244
14 E.g. There are an estimated 127,000 sight-impaired British Columbians over the age of 15. Reference #334.

Internet voting could have a significant impact on their ability to vote, and their ability to do so independently. There may also be other potential ways for election administrators to address these challenges (e.g. accessible voting machines in voting places).

Most implementations of Internet voting require voters to be registered to vote prior to casting an Internet ballot, and many require a second level of registration to qualify for Internet voting. Implementations of Internet voting that rely on authentication credentials being mailed to voters ahead of the voting period will not meet the needs of voters who are away from home for extended periods or do not receive home mail delivery.

Conclusion

Increased accessibility and convenience for British Columbia voters is the most significant potential benefit of Internet voting. Given the broader absentee voting opportunities available in the existing provincial electoral process, and considering the seasonal weather constraints for fall local government elections, the panel believes the potential benefits are greater for local government elections, but that they are also significant for provincial elections.

B.C. survey research into voter turnout has identified issues of convenience (e.g., too busy, out of town, family emergencies, illness) as the reason given for not voting by approximately one-third of respondents. This suggests that jurisdictions that offer Internet voting should see a significant increase in turnout over previous elections in those jurisdictions or over other comparable jurisdictions where Internet voting is not used. However, as described earlier in 4.1 - Increase voter turnout, the evidence does not show this.

4.3 Improve speed and accuracy of results[15]

Another commonly held view is that, because ballots are cast and counted electronically under Internet voting, tabulation with perfect accuracy is near instantaneous once voting closes. However, this perceived benefit is not always realized in Internet voting elections.

The Internet voting technology used in the 2012 Halifax Regional Municipality (HRM) elections required ballots to be digitally encrypted as they were cast in order to ensure the secrecy of the individual ballot and prevent anyone from being able to determine the results of any Internet ballots cast before the close of voting. After the close of Internet voting,[16] the process to mix[17] the 66,000 ballots took approximately half an hour. Due to the potential delay to the announcement of results if conducted on

15 For more information on this matter, see references #130, 131, 141, 187, 278
16 Internet voting was only available during the advance voting period
17 For more on mixing ballots cast on an Internet voting system, see Norway in Appendix F - Experience with Internet voting in other jurisdictions

election night, HRM chose to conduct this process at the close of Internet voting, ahead of election day, but did not produce the report that would indicate the tally of the votes until after all in-person voting was complete.

Similarly, an Internet voting pilot held in ten of 429 communities during the 2011 Norwegian Local Government Elections found that there was no statistically significant reduction in time required for the counting and reporting of results compared to control communities using traditional counting and reporting methods. While the Norwegian pilot used different technology and processes than HRM, it also found that processes unique to Internet voting meant that tabulation could not begin immediately upon the close of voting.[18] Further, there was "no relationship between the level of use of Internet voting and the time taken for the counting and results reporting process."[19] That is, contrary to expectations, even where Internet ballots were a higher proportion of all ballots cast, there was not a corresponding decrease in the amount of time it took for all ballots to be counted.

Although the time required to count and report results is not improved, the accuracy of counting and reporting can be.

While the provincial election ballot is fairly simple, election officials can sometimes make errors in the adjudication, counting and reporting of the several hundred ballots in their ballot box after administering voting for twelve hours. The complexity of the ballots used in local government elections compounds this issue. Internet voting enables a standard adjudication of ballots and precludes a potential variation between officials (anywhere from a few in a small local government community to thousands for a provincial election) and eliminates human error in counting, particularly when there are multiple ballots for officials to count or complex ballots are used. However, experience from provincial recounts shows a very low level of errors due to ballot adjudication and counting. For example, a recount in the electoral district of Saanich North and the Islands following the 2013 General Election found that only 13 of 31,697 ballots were adjudicated differently between the two counts, or were miscounted at the initial count.[20] Election administrators at both the local and provincial levels have a high level of confidence in the accuracy of current manual counting processes.

18 If a voter casts a ballot in-person it supersedes a ballot cast online, so Internet ballots could not be counted until it was determined that the voter did not vote in-person on election day. Dealing with ballot encryption also delayed the start of the Norwegian tallying. Reference #141.
19 Reference #141
20 Reference #256

The major speed issue in provincial elections relates to the gap between the initial count on election night and the release of the official results. Local government officials must release the official results by the end of the fourth day after general voting day. In B.C. provincial elections there is a legislated period of 13 days between the initial count and the beginning of the final count in which to process and count absentee ballots; such ballots may be cast until the close of voting on general voting day.[21] This additional time at the provincial level is required to ensure no multiple voting occurs under the current voting model. An Internet voting model added as an additional channel to the current system would not produce an earlier result.

Conclusion

Jurisdictions that have introduced Internet voting have had mixed results in terms of the speed in which results are available. At both the provincial and local government levels, preliminary results are typically available between thirty minutes and three hours after the close of voting. In local government jurisdictions where vote tabulation machines are already in use, results can be available even sooner. The panel feels that the existing speed and accuracy of results sufficiently meet the needs of voters, candidates, political parties and the media. Further, even if Internet voting results could be made available sooner, overall results for any election would still need to wait for the majority of votes that are cast on paper ballots to be counted by hand according to the traditional timeline.

While a standard adjudication of ballots could be an improvement, the panel trusts the accuracy of the existing manual counting processes.

The panel does not find the potential benefit of improved speed and accuracy of ballot counting, of itself, to be a compelling reason for the introduction of Internet voting as an additional channel at either the provincial or local government levels.

4.4 Cost savings of administering Internet voting over in-person voting[22]

For the 2013 Provincial General Election the cost of hiring election officials and renting voting places represented just over one-third of the total cost of administering the election. It is commonly advanced that Internet voting does not require the renting of voting places and the hiring of election officials and so a significant cost savings can be found over traditional in-person voting.

21 In both local and provincial government elections there is also a period after the announcement of the official results in which a judicial recount may be requested.
22 For more information on this matter, see bibliography references #76, 130, 131, 279, 337

However, this perceived financial benefit is based on Internet voting being used in place of traditional in-person voting opportunities. With only a few exceptions, jurisdictions that have implemented Internet voting have offered it as an additional channel of voting to supplement existing in-person voting. In these cases all costs associated with Internet voting are in addition to traditional expenses and, as a result, the total cost of administering the election increases.

Some jurisdictions have looked to partially offset the costs of adding Internet voting by reducing the number of in-person voting opportunities. This is because individuals who vote online will not need to attend a voting place and so fewer voting places and officials may be needed. Further, some officials hired may be needed for shorter periods of time as they are not counting ballots after the close of voting. For example, after initial success with Internet voting in 2008 and 2009, Halifax Regional Municipality believed that fewer voters would vote in person and so reduced the number of voting places for the 2012 election from 146 to 102 and the number of voting stations from 600 to 491. Such assumptions need to be carefully considered, as the Ontario City of Peterborough reported after its 2006 pilot that it had overestimated the impact of Internet voting on in-person voting and, accordingly, for the next election would need to hire more election officials for the voting places to reduce the long line-ups that resulted from the reduced staffing.

Internet voting also has the potential to reduce logistics and costs associated with the distribution of ballots and supplies around the jurisdiction. As well, Internet-only voting can facilitate late changes to the ballot to account for the inclusion or exclusion of candidates or political parties.

Conclusion

The panel considered three scenarios for implementing Internet voting having different consequences for the cost of elections.

In the first scenario Internet voting is grafted onto the current voting model as an additional channel. Under this scenario, there would be additional costs.

A second scenario is that as Internet voting is grafted onto the current voting model as an additional channel, the budget for the election is held constant, and the number of traditional voting places is reduced as a cost-saving initiative.

A third option is for a jurisdiction to offer Internet-only voting. This has the potential to provide significant cost savings over the traditional voting model.

The panel is of the view that if any Internet voting option is introduced in B.C., it should be done in a limited manner. Therefore, in the short- to medium-term, the panel believes that Internet voting provides little or no cost savings,

while recognizing that in the longer-term, if an Internet-only voting model were to be used, cost savings are possible. Elections Ontario considered piloting Internet and telephone voting in an Ontario by-election (approximately 85,000 voters) and reported that such a pilot "could cost close to $2 million".[23] British Columbia would have to conduct its own detailed cost assessment of a pilot project should it consider trialing Internet voting at either the local government or provincial level.

The panel does not consider the potential ability to make late changes to the ballot to be a determining factor in the consideration of Internet voting.

The cost of Internet voting is also seen by some to be a potential challenge (rather than a potential benefit) to implementing Internet voting. For further discussion of the issues related to the costs of implementing Internet voting, see Cost on page 39.

4.5 Require fewer resources of parties and candidates[24]

Just as in-person voting requires significant numbers of paid election officials to administer voting, in-person voting also places significant demands on candidates and political parties to find sufficient volunteers to attend the voting places and scrutinize the voting process. As political parties and candidates have increasing difficulty finding sufficient volunteers, the benefit of centralized observation of Internet voting becomes apparent. Instead of recruiting one volunteer for each ballot box in the jurisdiction, political parties and candidates would have to recruit sufficient volunteers and experts to audit the voting system.[25] Internet voting also makes it easier for candidates and political parties to identify in real time who has voted.

Conclusion

If Internet voting were to be the sole channel for voting it would reduce the amount of human resources required by candidates and political parties to scrutinize the electoral process, but if offered as an additional channel to in-person voting, Internet voting would, in fact, require more volunteers with different skills than at present. The panel does not think this is a compelling argument for introducing Internet voting.

23 Reference #232. For more information on Ontario's consideration of Internet voting, see Ontario in Appendix F - Experience with Internet voting in other jurisdictions
24 For more information on this matter, see reference #146
25 For more on the skills required to scrutinize Internet voting see 5.6 Transparency and auditability, page 33

4.6 Reduce/eliminate errors made by voters when casting ballots[26]

Another potential benefit to Internet voting is that technology can be designed to prohibit a voter from casting a ballot that has an error on it; that is, too many or too few candidates selected, unclear markings, or markings that identify the voter. Alternatively, the technology could still allow the voter to cast a ballot with an error to enable them to "spoil" their ballot after warning them that they are doing so.

In the 2013 Provincial General Election, 11,763 of all ballots cast were rejected. This represented 0.65% of the total number of ballots cast. It is not known whether these ballots were spoiled in error through incorrect markings by the voter, or whether they were spoiled by the voter in an effort to provide a statement on the election.

Conclusion

Internet voting has the potential to eliminate errors due to incorrect markings, but has no impact on ballots that are intentionally spoiled. The panel does not find the potential benefit of reducing or eliminating the number of errors made by voters when casting ballots to be a compelling reason for the introduction of Internet voting at either the provincial or local government levels.

4.7 Maintain relevance by keeping up with other aspects of society[27]

As the public becomes accustomed to using the Internet for other aspects of their lives there is an increased expectation that voting should be provided in the same way. Some researchers claim that if the methods for voting do not evolve in a manner similar to shopping, banking, socializing and playing games, voting may be pushed to the margins.

Other researchers have raised the opposite view and have described voting as having a unique role in a democratic society that merits retaining a different and distinctive set of procedures. This view suggests that voting is by definition a very public activity, and that it should occur in a public place, thereby emphasizing the community-based character of political participation. These views are reflected in anecdotal reports of Norwegian youth preferring to vote in person for social reasons.[28]

26 For more information on this matter, see references #48, 141, 146, 205, 338
27 For more information on this matter, see references #141, 231, 280
28 For more on the social preferences of Norwegian youth, see Norway in Appendix F - Experience with Interet voting in other jurisdictions

Some of these researchers also suggest that the actual costs of voting (attending a voting place for a few minutes every few years) are not an overly onerous component of the democratic system.

Conclusion

The panel recognizes the symbolic benefit of Internet voting as a way to maintain or increase the relevance of voting in our increasingly digital lives, but does not consider this benefit to be a significant one for B.C.

4.8 "Greener"[29]

Reducing the amount of paper required to print ballots and the amount of energy to distribute them across the jurisdiction is another perceived benefit of introducing Internet-only voting. Similarly, researchers suggest that Internet voting could also reduce the amount of fossil fuels burned by voters, election officials and scrutineers in travelling to and from the voting place by car or even public transit.

Conclusion

The panel recognizes the perceived potential environmental benefits of Internet voting, but did not evaluate the full environmental costs of Internet voting (including the energy required to power the computer systems and infrastructure) or the traditional voting channels and infrastructure and therefore does not take a position on the relative "greenness" of Internet voting.

29 For more information on this matter, see references #146, 215, 227

5.0 PERCEIVED AND ACTUAL CHALLENGES TO IMPLEMENTING INTERNET VOTING

Perception of the challenges or risks of implementing Internet voting differs among stakeholders. Vendors claim that the challenges have largely been overcome and the risks are minimal, whereas most technical experts state that ongoing concerns related to security are still to be resolved. While the public may desire to vote in a more convenient way, and some election administrators may desire to offer such conveniences, both groups do not always have all of the facts about the challenges of implementing Internet voting.

The kinds of risks involved in Internet voting are largely different from the kinds of risks faced in traditional voting opportunities. The degree of risk and the consequences of those risks also differ and need to be assessed. While there are accepted standards for assessing safety-critical systems generally, to date there is no common methodology for measuring the risks associated with Internet voting.

5.1 Security[30]

The challenge of providing secure Internet voting is perhaps the most significant of all the challenges the panel discussed.

In July 2013, a large group of notable American computer scientists wrote an open letter to a Virginia state legislative commission examining a Bill related to Internet voting stating that in their opinion "the technology necessary to support Internet voting, while also protecting the integrity of the election and voter privacy, does not yet exist."[31]

Broadly, there are three potential sources of security vulnerabilities in Internet voting systems:

- At the voter's device
- In transit
- At the election server

5.1.1 At the voter's device[32]

Most researchers and Internet voting solution vendors agree that the voter's device is the least secure of the three due to (1) the wide variety of devices used by voters, the efforts put into the maintenance of the software on those devices, and the technical background of those maintaining the devices, as well as (2) the lack of control over the voter's device by the election administration or Internet voting system vendor.

30 For more information on this matter, see references #83, 94, 95, 121, 144, 150, 203, 211, 213, 246, 247, 267, 272, 274, 281, 282

31 Reference #317

32 References in this report to the voter's "device" can be read as any means by which an individual could cast a ballot for Internet voting (e.g., computer, tablet, smartphone)

Personal computers are already the target of malware,[33] phishing attempts and other attacks. The precise amount of malware prevalent on computers is unknown and estimates (1-50%) vary widely within the security community. Researchers fear that existing malware that has been developed for other purposes such as capturing credentials used for online banking and purchases can be used to record the voter's authentication credentials or track who an individual has voted for. It is also possible that new malware written to target specific voting systems could track how an individual votes, or even alter how the ballot is marked, and that either activity could take place without the voter's knowledge. While malware is typically developed by individuals or small groups, state-sponsored malware is also believed to exist.

While anti-virus software can detect known malware, such software relies on threats being identified with sufficient time for an update to be developed that denies the effectiveness of the malware or removes it from the system. No anti-virus program can guarantee 100% detection of all fraudulent software. Most critically, protection against even known malware requires appropriate and up-to-date anti-virus software on every voter's device that is to be used for Internet voting. Despite the existing real threats of malware, use of regularly updated anti-virus software is not widespread.

Also, based on existing Internet security issues, Internet voting can be susceptible to phishing attempts and imposter websites. This refers to the practice of attempting to acquire authentication credentials or other personal information by posing as a trustworthy or legitimate entity. This often relies on users being directed to a fraudulent website that mimics the authentic site and thereby tricks the user into entering their credentials or other personal information. A forged Internet voting site could capture the voter's credentials and then present an error message to the voter that the voting site is temporarily unavailable, giving the creator an opportunity to use those credentials on the real Internet voting site.

There is also a concern that both malware and phishing attempts could be automated to enable creators to affect large numbers of votes with little manual effort. It is for this reason that Internet voting is seen as significantly more risky than existing in-person or even vote by mail opportunities that carry their own risks.

An individual's ability to vote depends on the security of their own device, for which the individual is responsible. While a means can be provided for the individual to check that their vote is counted, this would depend on the individual having a way to communicate and compute which is secure from the malware.[34]

It has also been reported that some personal computer hardware is not trusted to provide secure transactions.[35]

33 Merriam-Webster: malicious software; software designed to interfere with a computer's normal functioning (e.g., viruses, trojan horses, spyware)
34 For more on cryptography and voter verification, see 5.6 Transparency and auditability, page 33
35 Reference #274

5.1.2 In transit

Once a voter has cast an online ballot on a device, the contents of the ballot must be transmitted to the election servers over the Internet. The transmission of any data over the open Internet can be susceptible to attempts by third parties to read, intercept or modify that data if appropriate security measures are not taken. Secure protocols (e.g., SSL/TSL) do exist that can create a direct link between the voter's device and the election server. Encryption and digital signatures can also be used to protect the integrity and authenticity of the data in transit. Voter verification methods can also identify to the voter if the ballot has been tampered with.

5.1.3 At the election server

Distributed Denial of Service (DDoS)

A Denial of Service (DoS) attack is an attempt to overwhelm a server's capacity with traffic so that it is unable to perform its usual duties and respond to its intended users. A server subject to a DoS attack may respond very slowly to its intended users or appear unavailable altogether. A Distributed Denial of Service (DDoS) attack is a DoS attack that is conducted by a large number (thousands) of computers, typically controlled remotely through malware. A DDoS attack on an election server during a voting period could have the effect of making it very difficult, if not impossible, for voters to cast ballots online.

The Internet voting component of the 2012 federal NDP leadership election was the subject of multiple DDoS attacks during the voting period. The attacks caused the voting sites to be unavailable to most voters and the time for voting online had to be extended. While the Internet voting vendor stated that the target of the DDoS attacks (and therefore the failure point) was the political party website that directed voters to the actual voting page hosted by the vendor, and therefore the Internet voting servers were technically unaffected, the end result for the voter was still the same.

Some researchers state that DDoS can be mitigated by hidden or dynamic website addresses; however, this approach makes it more difficult for voters to confirm that they are at the legitimate Internet voting website and not a fraudulent imposter site because they are unable to match the website address they see against a known valid address.

It is partly the threat of DDoS attacks that leads jurisdictions to permit Internet voting for multiple days and only ahead of general voting day.

Remote intrusion

In order for voters to access the election server for voting, it must be available over the public Internet. This also makes the server accessible to anyone who wishes to try to break in to, or compromise, it. Nearly every major website has been compromised, including the U.S. Department of Defence, Google, the FBI, and various financial institutions. Internet voting servers are likely no more secure than these major financial and government servers.

While no Internet voting server has reportedly been compromised during an election, Washington D.C. election servers were successfully compromised by a professor and a group of graduate students from the University of Michigan during a public test of the system's security. Ahead of the 2010 D.C. election, administrators invited the public to test the security of its system in a mock election scheduled for the month prior to an actual election in which Internet voting would be used. The University of Michigan group was able to take advantage of flaws in the system's source code and poor security management implementation (e.g., not changing default passwords to associated systems) to completely compromise the integrity of the Internet voting system. The group was able to add fraudulent ballots, change the results of previously cast ballots, and observe how voters were voting without being detected by the election officials, or by the firm engaged to audit the voting process. Based on the complete failure of the security, the Internet voting component of the 2010 election was cancelled.

One of the most critical technical challenges is detecting a compromise of a voting system. The state of the technology today is such that it is virtually impossible to guarantee that an intrusion would be always detected. It is also virtually impossible to guarantee that a voting system has not been compromised during an election. The risk is significant, as a compromise of a voting server can lead to a large-scale fraud.

Insider threats

There is also a risk that an insider could have access to results as votes are cast, be able to change results, or be able to associate ballots with specific individuals. Systems need to guarantee that no individual, including election administrators and system technicians, can compromise the secrecy of any ballot cast. Votes must be encrypted in a way that prevents any single individual from decrypting individual ballots. The key to decrypt the votes can be broken into pieces and shared among multiple individuals or stakeholders, of which a minimum number of pieces must be used to decrypt the ballots for counting.

To prove that the integrity of an Internet voting system has not been compromised by an insider through inserted code, Internet voting systems are typically assessed by contracted auditors and experts.[36]

36 For more on maintaining the integrity of software code see 5.6 Transparency and auditability, page 33

Conclusion

While there is no evidence that an election making use of Internet voting has been successfully compromised, this is not proof that it has not occurred, only that if it has occurred it has not been detected. The Washington D.C. example discussed above illustrates that an undetected compromise is possible. However, this argument could be applicable to all elections, including those that use traditional voting channels.

Some of these security issues could eventually be resolved by advances in hardware and software tools.

Although traditional voting is not without risk, it is much harder to perform and conceal large-scale fraud in traditional voting than in Internet voting. Policy-makers must decide what is an acceptable level of risk to a jurisdiction.

5.2 Compromised election results[37]

From banking and the purchase of goods and services, to communicating with friends and the public at large on social networking sites, the Internet is used for a wide variety of transactions by British Columbians every day. When those transactions are affected by security breaches and fraud, users may temporarily or permanently lose money (depending on whether those transactions are guaranteed by a financial or credit institution), be the subject of identity theft, or have their individual reputations tarnished by communications purportedly made on their behalf.

In comparison, the consequence of an election being affected is significantly higher than most Internet transactions if the wrong candidate or political party is elected with the ability to exercise the functions and powers of government.

It is easier for a smaller number of people to have a larger effect on votes in an Internet voting election than a traditional in-person election. Instead of having to corrupt the process for one voter at a time, automation of the processes allows for the automation of that corruption. Further, those wishing to have an effect on votes do not need to be present in the jurisdiction.

It has been suggested that some jurisdictions are not large enough targets for individuals or organizations looking to compromise an Internet voting system, and therefore the consequences of introducing Internet voting in those jurisdictions are less. However, the discovery of a vulnerability in one jurisdiction may increase the risk of that vulnerability being used in any other jurisdiction that uses the same technology, regardless of the size of the jurisdiction.

37 For more information on this matter, see bibliography references #121, 247, 281

The risk is even greater when there are a limited number of vendors serving all jurisdictions. Further, since security vulnerabilities can be purchased, the individual or group interested in compromising a system does not need to have discovered the vulnerability themselves.

Permitting Internet voting only ahead of general voting day and requiring pre-registration are seen as mechanisms to reduce the consequence of a security breach or other failure of the Internet voting system.

Conclusion

While the panel acknowledges that higher profile elections may make more attractive targets to individuals or groups looking to affect an Internet voting result, the panel believes that the election of the wrong candidate or party in even the smallest community in British Columbia is a serious matter.

5.3 Accessibility, usability and availability[38]

Unlike many other Internet transactions, the period for conducting an election is legislated. This means that Internet voting systems must be available to voters at precise times and voting cannot ordinarily be delayed if systems are compromised.

In traditional elections it is rare for a problem to occur that affects voters beyond a single voting place or community. However, a problem with an Internet voting system, such as a Distributed Denial of Service (DDoS) attack, could potentially impact all eligible voters. While the Chief Electoral Officer (for provincial elections) and the Minister responsible for the *Local Government Act*, chief election officers and presiding election officials (for local government elections) have the authority in law to extend or alter key dates of the election in exceptional circumstances, any changes would be difficult and expensive to communicate to voters. For this reason, most jurisdictions offer Internet voting over an extended period of time, prior to general voting day, and as an additional opportunity for voting rather than the sole option.

While Internet voting systems have the potential to improve services for voters with disabilities, these systems need to be compatible with a wide range of commonly used accessibility software and hardware by these voters in order for this benefit to be realized.

Increasing the security of an Internet voting system can increase the complexity of the system which may in turn reduce the usability of the system by voters. This is particularly a concern for voters with low technical capabilities or literacy levels.

38 For more information on this matter, see references #48, 121, 142

Researchers also speculate that if Internet voting replaces existing voting opportunities it risks creating a "digital divide" in which those without (or with reduced) Internet access have less access to voting than others.

Conclusion

Compatibility of the Internet voting system with widely used accessibility software and hardware needs to be considered if Internet voting is to be a benefit for voters with disabilities that encounter challenges with the traditional voting processes.

Provided traditional voting opportunities are maintained, the digital divide is not a significant concern for the panel.

The panel considers the specific issues of accessibility, usability and availability of Internet voting to be challenges that can be largely overcome or mitigated by jurisdictions if they consider these issues early in the planning phase prior to implementation.

5.4 Authentication and ballot anonymity[39]

Authentication and anonymity are two opposing, but interrelated, concepts. To ensure a voter is eligible and only votes once, the individual requesting a ballot must be confidently authenticated by the election administration; however, once authentication is confirmed, the voter's identity must be disassociated from the ballot to ensure the principle of the secrecy of the ballot is maintained.

Under traditional in-person voting processes, authentication occurs in a face-to-face transaction where the voter uses identity documents or other methods to satisfy the voting official as to the voter's identity and place of residence.[40] Anonymity is protected by giving all voters an identical ballot with no personally identifying markings and asking the voter to place the marked ballot in a ballot box where it is mixed with all other ballots before the box is opened at the end of the voting period and counted.

Authentication

When authentication occurs remotely, traditional identity documents must be replaced with another form of credential that can be used and verified electronically. In order to assign such credentials to the voter, the election administrator must know with a high degree of confidence who the voter is and whether they are entitled to vote.

39 For more information on this matter, see references #48, 94, 121, 139, 140, 180, 190, 207, 231, 258, 286

40 While some voters may vote using absentee voting processes, most of these opportunities also take place in public under the eye of candidate representatives who scrutinize the process. Only voters who cast ballots by mail are authenticated differently. For more on this issue, see 5.6 Transparency and auditability, page 33.

Most jurisdictions that offer Internet voting require some form of pre-registration prior to allowing an individual to vote online. This enables the election administration to compare registration to existing voter authentication data. In some places, simply being a registered voter in the jurisdiction is sufficient but, in others, Internet voting requires a separate Internet voting registration process. In either case, individuals who have not previously registered to vote or applied to vote online will be unable to cast an Internet ballot if they wait until the last minute. While Internet voting can be a method of increased convenience for voters, it still requires some prior planning in order to be used.

There are various ways that authentication credentials can be provided to voters, depending on how Internet voting is implemented. Many jurisdictions that have a high level of trust in the postal system will mail the credentials to all eligible Internet voters ahead of the voting period. Credentials vary, but often take the form of a unique Personal Identification Number (PIN) or passcode. Depending on whether there is a second level of Internet voting registration, the voter may then use that PIN online, typically in combination with the voter's date of birth or another "shared secret",[41] to register to vote electronically or to vote directly. When a second level of registration is required, the voter is given a new PIN either during the online registration or subsequently in the mail. The voter may also have the opportunity to create their own password that will be used in combination with the provided PIN in order to vote.

Once credentials have been provided to voters, the election administration must still be assured that the person using the credentials is the person to whom the credentials were issued. Requiring the voter to provide a shared secret in addition to what is mailed is one way to reduce the risk of impersonation, but some shared secrets such as date of birth are not as secret as they were once considered to be. While requiring a date of birth may be a reasonable way to prevent the average person who intercepts the mailed credentials from using them to vote on the voter's behalf, family members and close acquaintances may also know that shared secret, particularly with the increased disclosure of birth dates through social media.

In any form of remote voting outside of the relative protection of the voting place, voters are more susceptible to attempts of intimidation and improper influence of the voting intentions. This applies to both Internet voting and traditional vote by mail provisions.

In some jurisdictions citizens already have electronic credentials that are used for accessing other government services and can also be used by eligible voters for Internet voting. This eliminates the need for the election administration to provide unique credentials. These credentials that are used for multiple purposes are less likely to be lent or sold for the purposes of allowing someone else to cast a ballot on the voter's behalf.

41 Term for a fact or idea that both the voter and the election administration know, but that few or no other individuals will know.

Voters are also more likely to keep them safe. However, the longer the same authentication mechanism is used, the more likely vulnerabilities in the authentication mechanisms will be discovered.

British Columbians do not currently have electronic credentials for accessing government services. The Ministry of Technology, Innovation and Citizens' Services has developed a new foundational identity document called the BC Services Card to combine the BC Drivers' Licence or BCID card and BC CareCard. This new card contains enhanced security and privacy components and has the potential to be used for secure authenticated interaction with government services, including some services offered online. The card is being distributed to eligible[42] B.C. residents on a five-year rolling basis from 2013 to 2018. The authentication capabilities have yet to be implemented.

Ballot anonymity

Ballot anonymity refers to the inability to link a ballot with the individual who cast it. This is directly related to the principle of the secret ballot (below) and the security of the Internet voting system (above). In contrast to in-person voting where identical paper ballots are placed in physical ballot boxes where they are mixed with all other ballots prior to counting, the connection between the voter's identity and the content of the ballot cast electronically is fundamentally and necessarily linked for both technological and policy reasons. The order in which the ballots are cast, stored by the system and eventually counted will match the order in which voters were marked as having voted, and unless these linkages are broken somehow, it would be possible to identify a voter with their ballot. Further, when voting systems allow voters to cast multiple ballots[43] the Internet voting system, and therefore election administrators, must be able to identify which ballots have already been cast by the voter so that the subsequent ballot replaces the previous ballot. If the link between the ballot and the voter is broken before the end of all voting, this cannot be done.

The absentee voting process used in B.C. provincial elections and for mail ballot voting in B.C. local government elections provides authentication and anonymity through a double-envelope process.[44] Digital versions of this process exist for Internet voting.

42 B.C. residents aged 19-75

43 For more on this matter, see Norway in Appendix F - Experience with Internet voting in other jurisdictions

44 The marked ballot is placed in an unmarked "secrecy" envelope. The secrecy envelope containing the ballot is placed in an outer "certification" envelope that identifies the voter. At the conclusion of voting, the certification envelope is examined to ensure the voter was eligible to vote and has not voted at another voting opportunity. If the voter was entitled to vote via the absentee process the certification envelope is opened and the secrecy envelope is removed from the certification envelope. The secrecy envelope is placed in an unmarked ballot box and the certification envelope set aside. Once all absentee ballots have been reviewed in this manner, the ballot box containing the secrecy envelopes is shaken to shuffle the secrecy envelopes. That ballot box is opened and each secrecy envelope is opened. The ballots are separated from the secrecy envelopes and placed into a new ballot box, which is then shaken to mix up the order again. The ballots are now two steps removed from the certification envelope that listed their identity and so can be counted per the ordinary ballot counting process.

It is possible that over time the current encryption methods will be broken and any public voter validation codes could be used to identify how individuals that used those encryption methods voted in past elections.

Conclusion

The panel considers authentication to be a key issue for jurisdictions considering Internet voting.

While two-step authentication methods can be more secure than single step authentication, such processes are more complex to administer and for voters to use. Two-step authentication models also require additional forethought by the voter ahead of voting thereby reducing convenience.

However, if the BC Services Card works as promised, authentication could be a less significant issue. If the BC Services Card were to be considered as a secure authentication credential for Internet voting, Internet voting vendors and the B.C. government would need to collaborate to ensure the two systems could work together.

Any Internet voting option should provide for anonymity using properly implemented secure methods.

5.5 Secrecy of the ballot[45]

The secret ballot is a tool to protect the freedom of voting. Secrecy prevents third parties from knowing how an individual has voted, which prevents vote buying and voter coercion. Unsupervised voting (e.g., vote by mail and Internet voting) is more susceptible to vote buying and coercion than in-person voting because it cannot be guaranteed that voters are casting their ballots alone.

Researchers disagree as to precisely how the principle of a secret ballot should be interpreted. Some claim that the law must prevent voters from voting in a way in which the level of secrecy is reduced. Others claim that the principle only requires the opportunity for a secret ballot, while allowing for voters to choose less secret options. Most Canadian policy-makers (including those responsible for provincial and local government election policy in B.C.) have accepted the reduced level of secrecy offered by vote by mail in order to provide a more accessible voting process. Voters who need assistance marking their ballot in a voting place, either from an election official or a friend or family member that accompanies them to the voting place, also sacrifice some secrecy in return for the ability to vote.

The level of secrecy afforded to Internet voters depends on the specific form of Internet voting implemented in the jurisdiction.

45 For more information on this matter, see references #7, 130, 142, 180

If the voter is required to use the voter's ID card or drivers licence, the voter will be less willing to provide it to someone else because it has other uses. If the mechanism for authentication is not valued highly by the voter (e.g., a one-time-use PIN distributed by election administrators and not tied to other uses), the likelihood of selling or transferring the authentication credentials increases.

Some jurisdictions permit voters to cast multiple ballots, with only the final ballot ultimately being counted. This technique attempts to counter the impact of an influenced vote by enabling the voter to replace the influenced vote with a subsequent one that is cast free of influence (either online or in-person). Not only does this enable the voter to achieve the right to a secret ballot, it reduces the incentive to buy a vote in the first place because the purchaser cannot guarantee that the ballot they observed being cast will be the ballot that gets counted.

Traditional voting opportunities protect the secrecy of the ballot at the expense of the voter being able to have confidence that their vote has been included in the tally of votes for the candidate of their choice. This is accepted as a reasonable trade-off in Canada as ballots are fairly simple to mark correctly[46] and voters have a high level of trust in the election officials to interpret and count their ballot correctly. Internet voting systems that incorporate end-to-end verifiability[47] enable the voter to have a higher degree of confidence that their vote was counted as they intended.

Conclusion

The panel acknowledges the reduced level of secrecy offered by all remote voting opportunities, including Internet voting and voting by mail. That risk, for voting by mail, is mitigated by the fact that voting by mail is done by a very small fraction of the electorate. Risks to secrecy for Internet voting could occur on a wider scale if Internet voting was more widely adopted.

Internet voting implementations that permit voters to cast multiple ballots to counter the effects of improper outside influences, provided that only one vote is counted for a single voter, may mitigate this risk, as would ending the availability of Internet voting ahead of general voting day and establishing that any paper ballot cast by a voter would supersede an Internet ballot cast by the voter.

While Internet voting systems that provide a receipt[48] contravene the strict principle of a secret ballot by enabling the voter to prove to another individual how the voter voted, the panel does not consider the likelihood of voter coercion or vote selling to be high if this is implemented in B.C. In a new

46 In the 2013 Provincial General Election approximately 0.65% of ballots were rejected. For more information on this matter, see 4.6 Reduce/eliminate errors made by voters when casting ballots, page 20.

47 For more on end-to-end verifiability, see 5.6 Transparency and auditability, page 33

48 For more on the use of receipts, see 5.6 Transparency and auditability, page 33

Internet voting system that uses a receipt, it may be necessary to reduce the level of secrecy in return for an increased level of trust.[49]

5.6 Transparency and auditability[50]

In B.C. and most jurisdictions, candidates are entitled to appoint representatives (commonly referred to as scrutineers) to attend the voting place on their behalf and observe the registration, voting and counting processes. They are entitled to witness the activities of the election officials and voters and ensure that the requirements of the applicable laws are followed and that the process is administered consistently and fairly. They may record who has voted and report this to their campaigns and, after monitoring the counting process, take a copy of the official results for each ballot box back to their campaign. While they may not know the intimate details of the election laws, most eligible voters are familiar enough with the traditional in-person voting process and underlying principles to act as scrutineers at a provincial or local government election in B.C. Many jurisdictions also allow for independent observers to monitor the processes. This ability to scrutinize the registration, voting, and counting processes is a key aspect of a transparent electoral system.

Reviewing and evaluating Internet voting and electronic counting is very different from scrutinizing in-person voting and counting. Since voters are authenticated and ballots are cast remotely, observers cannot monitor the casting of individual ballots. Instead, observation of Internet voting usually involves the review and evaluation of the hardware, software and processes involved in administering the online voting before voting takes place. This type of observation is sometimes referred to as auditing. These reviews require specialized skills and knowledge that significantly limit who can perform them. Some Internet voting systems also have audit functions built into the software to allow for independent review and evaluation while voting takes place. Such functions can include the ability to see a live list of who has voted and even log in and cast "audit ballots" using the same processes as voters to ensure that the system is performing appropriately.[51]

Many election authorities rely on an outside individual or organization to act as an auditor for the entire Internet voting process on behalf of both the election administration and the candidates and political parties. Anyone acting as an auditor for an Internet voting process must be capable of performing appropriate process audits and the election administrator must be capable of understanding the results and limitations of those audits.

49 For more on trust, see 5.7 Trust, page 37
50 For more information on this matter, see references #27, 94, 142, 144, 156, 167, 195, 206, 228, 254, 286, 310
51 Audit ballots are specially marked ballots that would not be counted with ordinary ballots and so would not affect the results of the election.

Despite the reliance on outside auditors, most vendors state that any authorized individual would be entitled to review the system under a non-disclosure agreement (NDA). As most commercial Internet voting systems are built with proprietary technology, Internet voting vendors typically require those reviewing, certifying or auditing its systems to sign a non-disclosure agreement limiting what the subject can share publicly. These restrictions can be seen to reduce the level of transparency to the entire process.

To balance this lower level of transparency and maintain trust, policies, procedures and system documentation need to be available to participants and opponents alike.

The Norwegian election administration released the source code for its Internet voting systems in summer 2013 in order to inspire trust, enhance transparency and enable verification of its security by all experts, rather than just those willing to sign an NDA. The Estonian election administration released most of the source code for its Internet voting systems. However, the most security-critical portions of the code were not released and therefore a complete security assessment by outside experts was not possible. Open source code can permit any individual with the appropriate skills to review the software that is used and identify flaws in the code in order that such flaws come to light faster. In order to be run by a computer, source code must be compiled and translated into machine code. This process can also introduce errors that would be difficult to detect.

A complete assessment of all software code, systems and processes is very time-consuming and requires a high level of specialized skills and knowledge. Such a review would need to be conducted sufficiently ahead of the scheduled election so that any problems identified in the review could be rectified, and retested. Such thorough reviews could also prove to be expensive. There is currently no recognized standard for Internet voting technology to be evaluated against, either in Canada or internationally. However, components of these systems, such as the cryptography used, can be evaluated against well-established international standards.

An audit is "an independent pre- and/or post-election evaluation of an organization, system or process which includes quantitative and qualitative analysis."[52] Auditability refers to the degree to which the integrity of the overall system (technology and processes) and, ultimately, the results of the election can be confirmed. Thought of most broadly, this could include a review and certification of the hardware, software (including source code) and processes used by the Internet voting vendor and election administration prior to use, monitoring of those systems and processes during use, and evaluation of those systems and processes after use.[53] However, no standards for measuring the quality of such monitoring currently exists.

52 Reference #235

53 Systems must be monitored as soon as they are brought online (and therefore subject to attack), not just once voting begins.

In practice, third party audits of Internet voting systems are typically quite limited in scope. The audit report of the 2012 Halifax Regional Municipality (HRM) Internet voting system mentioned below specified that the application of the "Specified Auditing Procedures" established by HRM "[did] not constitute an audit or review engagement and, accordingly, no assurance is expressed." The reference to this statement here is not meant to pass judgment on the process used in Halifax or imply that the audit raised specific concerns or that the results were not accurate. It is raised here only to highlight an example of the limited scope of these observations characterized as audits and illustrate that they do not necessarily provide the same level of confidence that lay individuals may infer from the term "audit" and the reputation of the firms involved.

Auditability can also simply refer to the degree to which the results can be independently confirmed. Paper ballots can be recounted if requested by a candidate, if process dictates by an election administrator, or if ordered by the courts. Such a recount is easy to follow visually and the results of the initial count can be independently confirmed or overturned.

When votes are cast electronically, there are no physical representations of the ballot to be manually counted. Instead the system tallies the results from each electronically recorded ballot and generates a report of those totals. To recount those ballots means to regenerate another copy of the same report based on the system's existing interpretation and record of how those ballots were cast. Because they are based on the same underlying information, the regenerated report will always provide the same results as the initial tally.

For example, when a close result in a 2012 Halifax Regional Municipality election triggered a requirement for a judicial recount, the bylaws governing that election required that the election administrator provide a copy of the regenerated results report to the court and those results were added to the judge's count of the paper ballots. The election administrator also provided a copy of a third party auditor's report that confirmed that the tally of the system's interpretation of each ballot was correct. Such an audit does not determine if the system recorded the voter's intention accurately in the first place.

Due to the nature of how Internet ballots are cast, the concept of a recount under an Internet voting system shifts from a reconsideration of each ballot that was cast to an audit of the integrity of the system and processes by which those ballots were cast. This is a fundamental change to how stakeholders currently view the process.

Some Internet voting systems employ protocols commonly referred to as end-to-end verifiable (E2E) cryptographic systems. They are designed to answer three questions:

- Was the ballot marked as intended?
- Was the ballot collected by the system as the voter marked it?
- Was the ballot counted as the voter cast it?

While E2E systems enable anyone to tally the results and confirm that all votes were cast by eligible voters, they also generate new challenges for the voting process. Most significantly, they require voters to take further action after casting their ballot if they wish to verify the integrity of the system. This takes additional effort and adds another level of complexity to the process for the voter.

Even if used fully by voters, E2E systems are not the panacea to the issue of Internet voting security. E2E systems do not help when authentication credentials have been used by a third party. Malware could change the voter's intent if the voter uses an unsecured device, although an E2E system could enable the voter to detect such tampering. Depending on the implementation of the voter verification process, some E2E systems that provide voters with a receipt can enable a voter to definitively prove how they have voted, but this compromises the principle of a secret ballot and allows for coercion.

Perhaps the most significant challenges related to E2E systems that can prove tampering occurred are related to matters of public policy. How can tampering be distinguished from voter error (e.g., voter selects the wrong candidate)? What happens if evidence of tampering is identified? How much tampering must be identified to call the entire Internet vote into question? What is done when the Internet vote is called into question? Do all Internet ballots get disqualified? May affected voters cast a replacement ballot in-person? When does this determination get made? What happens if evidence of tampering is found after results are announced? If multiple jurisdictions use the same system concurrently, does tampering in one election affect decisions about the other?

Conclusion

The panel believes that the ability of parties, candidates and smaller jurisdictions to effectively audit an Internet voting process is quite limited and may in fact need to be outsourced. How these entities employ others to do this could conflict with vendor restrictions on access to proprietary systems, source code and documentation. At the local government level it may be necessary for multiple jurisdictions to work together, or perhaps with the provincial government, to develop a centralized oversight and auditing body. While better than relying on vendor assurances, these reviews are still no guarantee that the systems work as promised.

Whether or not the existing process is actively overseen, the capability to oversee the voting and counting process is there, and in a far different manner than an Internet voting system. Internet voting shifts the nature of oversight from individual ballots to the system as a whole.

The panel believes encryption and individual and independent verifiability (e.g. end-to-end verification) are key factors in assessing Internet voting and should be considered important aspects of ensuring transparency and auditability by any jurisdiction considering the implementation of Internet voting.

5.7 Trust[54]

When radical changes are made to known and trusted processes there is a significant risk that a degree of trust will be lost at least temporarily and will need to be re-earned. Introducing Internet voting, even as a complement to existing voting opportunities, can be such a radical change. In contrast to traditional voting processes, the level of knowledge about Internet voting processes is very low and this lack of knowledge creates distrust. If the losers in an election and their supporters do not trust that they lost fairly, the legitimacy of the elected government is in jeopardy.[55]

Voters trust local government chief election officers and Elections BC to administer elections in a manner that is fair and in accordance with the applicable laws. Public confidence in the electoral process and the legitimacy of elected officials in British Columbia is high. This legitimacy of elected officials and the government of the day are fundamental to our democracy. If an election conducted using Internet voting is compromised, or even suspected to be compromised, the legitimacy of the elected government is at stake.

When voters cannot easily observe the voting process and laypersons are replaced by information technology experts in the administration of voting, the level of trust is also affected. There may also be a fear of the "privatization of democracy."[56] Ways to generate trust include: ensuring that information is made available about the Internet voting system; ensuring proper testing, certification and audit mechanisms are in place; and implementation of an independently verifiable and evaluated system.

Conclusion

There currently exists a high level of trust in local government and provincial elections in B.C. Many of the other challenges outlined in this report can affect the level of trust stakeholders will have in an Internet voting system, and the ability of an election administration to satisfy those challenges is a key determinant in the level of trust stakeholders will have in an Internet voting

54 For more information on this matter, see references #142, 167
55 For more on this matter, see 5.2 Compromised election results, page 26
56 Reference #167

system. However it is important to note that not only should stakeholders perceive the election system to be trustworthy, but the election system should in fact be trustworthy. Trust in an election system comes from developing a system that is trustworthy.

The panel acknowledges that when first implemented, Internet voting will not have the same level of trust as the existing voting processes, but wholeheartedly recommends that jurisdictions considering the implementation of Internet voting take all reasonable efforts to build as high a level of trust as possible with stakeholders and to begin doing so as early in the planning phase as possible.

5.8 Stakeholder management[57]

The introduction of Internet voting introduces a new stakeholder in the electoral process – the Internet voting technology vendor. In order to work effectively with, and maintain control over, the vendor, election administrators must become, or surround themselves with, technology experts. If election administrators fail to do this they will effectively delegate oversight of the election to the technology vendor.[58]

Election administrators must educate voters, work with opponents of Internet voting and learn how to address public concerns.

Election administrators themselves may also need to build a refocused skill set that includes management of technology implementation and increased focus on open information policy in order to build and maintain trust in Internet voting.

Conclusion

Some vendors the panel heard from claimed that election administrators implementing Internet voting would need only minimal technical expertise within their organization. The panel feels that vendors may underestimate the significance of election administrators delegating oversight of the key elements of an Internet voting election to a technology vendor. Election administrators must retain sufficient oversight capability to identify vulnerabilities that a vendor may not want to disclose for business or competitive reasons. Given the variation in how elections are administered in B.C., the panel also questions whether vendors have sufficient capacity to manage a large number of new clients while still providing a high level of service.

The panel recognizes that developing adequate technical expertise and maintaining control over the technology vendor and ultimately the electoral process will be more difficult in smaller jurisdictions without assistance from the provincial government or other jurisdictions having the required technical expertise.

57 For more information on this matter, see bibliography reference #142
58 Election administrators must avoid simply delegating such oversight to technology contractors.

At the provincial level the administration of Internet voting would likely be centralized. This may change the nature of the relationship between the candidates and Elections BC. Instead of working almost solely with the District Electoral Officers in the electoral districts on issues related to the voting process, candidates and their campaigns would likely want to have, as well, a closer relationship with Elections BC headquarters staff managing the Internet voting technology.

5.9 Cost[59]

While some see Internet voting as a way to reduce the costs of election administration, Internet voting is usually offered as an additional channel for voting and therefore increases the total cost of election administration.[60]

Further, Internet voting introduces numerous new activities beyond the administration of voting that also will require budgeted funds and significant amounts of time. These include: developing and implementing an effective communications strategy to inform and educate voters about the new voting opportunities and voting processes;[61] a comprehensive evaluation of the Internet voting system, including a review of all hardware and software (e.g., source code) and mock elections, well ahead of implementation; and a thorough audit and review of the system and processes after the election. Some of these activities may be one-time costs that could be amortized over multiple elections, but others will be necessary each time an Internet voting election is held. Some activities that appear to be one time costs (e.g. source code analysis and penetration testing) may actually become ongoing costs, because even if the system has not changed since it was last used, the skills and motivations of potential attackers will evolve over time.

The precise costs of implementing Internet voting are not easily determined. Jurisdictions do not account for, and report, costs associated with elections and Internet voting in a consistent manner.[62] Due to these significant differences the panel could not do an "apples to apples" comparison and therefore did not attempt to determine the specific costs of implementing Internet voting for either provincial or local government elections in British Columbia.

59 For more information on this matter, see references #48, 121, 144, 146, 195, 217, 227, 290, 292

60 See 4.4 Cost savings of administering Internet voting over in-person voting, page 17

61 Elections Ontario's recent research into Internet voting "indicated that the communications and outreach materials represent approximately 10% of the budget for implementing [Internet voting]." Reference #292.

62 For example, the City of Markham claims a "cost per elector" of $0.81 for Internet voting in its 2010 municipal election compared to $5.63 for in-person voters. It is unclear if those published costs of Internet voting include all of the marginal costs of adding Internet voting to an existing election (e.g., costs associated with producing and distributing authentication credentials by mail, public information campaigns associated with Internet voting, etc.), or just the service contract with the vendor. It is also unclear whether the cost per in-person voter includes all costs related to Markham's election administration, or strictly the costs attributable to in-person voting (e.g., voting place rental, staffing, printed supplies, etc.).

Internet voting system vendors typically charge on the basis of a cost-per-registered voter and not based on the number of voters who choose to use Internet voting in the election. This means that the cost of the service can be determined ahead of time. It is unclear to the panel whether this cost model depends on a minimum number of registered voters.

Developing an Internet voting system and selling the service of administering Internet voting is still a relatively new business. It is not known whether the amount charged by vendors today represents a stable cost over time, or whether it is being offered at a reduced rate in order to acquire customers and could increase over time.

A jurisdiction considering Internet voting must decide between purchasing the services of one of a limited number of vendors and developing its own Internet voting system. Purchasing the existing services of an Internet technology vendor is seen to be significantly less expensive than a jurisdiction developing its own Internet voting system. When determining whether to purchase the services of a vendor or develop an in-house system, the impact on system security will also need to be considered. All Canadian jurisdictions that have used Internet voting have purchased the services of one or more vendors. Estonia, Geneva and Norway are three of the more well-known jurisdictions that have developed their own Internet voting system.[63]

Conclusion

The precise costs associated with implementing Internet voting will highly depend on the size of the jurisdiction (number of registered voters), the existing capacity within the jurisdiction to manage this new process, and whether the jurisdiction develops a new system or purchases the services of an Internet voting system vendor.

Developing an Internet voting system is more expensive at the outset, and possibly over time, than purchasing the services of an existing vendor. However, with the additional cost to develop a new system comes an increased flexibility to design a system that meets the specific needs of the jurisdiction and a potential for increased transparency. Policy-makers will need to determine whether the financial costs of developing a new system outweigh any benefits. The panel does not believe that any local government in B.C. could afford to develop its own system without the assistance of the provincial government and would almost certainly need to purchase Internet voting services from a vendor.

In any case, jurisdictions considering implementing Internet voting must recognize that there are significant financial costs to the decision beyond the Internet voting system contract.

63 For more on the Canadian and international jurisdictions that have used Internet voting, see Appendix F - Experience with Internet voting in other jurisdictions

6.0 SUMMARY

After this review, the panel notes that the benefits of Internet voting are not as persuasive as one might initially think. The panel also recognizes that policy-makers and election administrators will need to seriously consider the ability of each jurisdiction to satisfy the challenges posed by introducing Internet voting. The following represent the panel's assessment of the perceived and actual benefits and challenges to implementing Internet voting at the local and provincial government levels.

6.1 Perceived and actual benefits

Increase voter turnout:

- Evidence is mixed, at best
- Not convinced Internet voting will result in increased turnout at either level in the long run
- Not a compelling reason for introducing Internet voting

Increase accessibility/convenience:

- Most significant potential benefit for B.C. voters
- Potential benefits greater for local government elections due to seasonal weather constraints for fall elections
- Fewer potential benefits for provincial elections due to broader existing absentee voting opportunities
- Most compelling reason for Internet voting

Improve speed and accuracy of results:

- High level of confidence by election administrators at both levels in current counting methods
- Speed of overall results still dependent on hand-counted paper ballots (unless Internet voting is only channel)
- Preliminary results already reported quickly on election night for both local government and provincial elections
- Not a compelling reason for introducing Internet voting

Cost savings of administering Internet voting over in-person voting (see also Cost on page 44):

- Opportunities for cost savings require Internet as only option
- As an additional channel, Internet voting will result in increased costs
- May be possible to offset some Internet voting costs with reduced in-person voting

- More costs to consider than the contract with the vendor or initial development of system in-house
- Not a compelling reason for introducing Internet voting, at least in the short to medium term

Requires fewer resources of parties and candidates:

- Fewer volunteers possible if Internet voting is only option
- As an additional channel, more volunteers required
- Volunteers need different skills under Internet voting
- Not a compelling reason for introducing Internet voting

Reduce/eliminate errors made by voters when casting ballots:

- Potential to eliminate errors due to incorrect markings
- No impact on ballots that are intentionally spoiled
- Not a compelling reason for introducing Internet voting

Maintain relevance by keeping up with other aspects of society:

- Symbolic potential benefit not considered significant for B.C.
- Not a compelling reason for introducing Internet voting

Greener:

- Relative "greenness" unknown without full evaluation of both Internet voting and traditional voting

6.2 Perceived and actual challenges

Security:

- Potential for large-scale fraud is greater for Internet voting than traditional voting opportunities
- Policy-makers must decide an acceptable level of risk to a jurisdiction

Compromised election results:

- Higher profile elections may make more attractive targets
- Consequences likely higher at more senior levels of government
- Election of wrong candidate or party in even the smallest community a serious matter

Accessibility, usability and availability:

- Compatibility with accessibility software and hardware needs to be considered
- Digital divide not a significant concern
- Can be largely overcome if considered early enough

Authentication and ballot anonymity:

- Key issue for jurisdictions considering Internet voting
- Two-step authentication can be more secure, but also more complex for administrators and voters
- BC Services Card could make authentication a less significant issue if considered secure and can be incorporated into an Internet voting system

Secrecy of the ballot:

- All remote voting opportunities offer reduced degree of secrecy
    - Use of vote by mail very low at both levels
    - If Internet voting widely adopted, this risk increases
- Effects of improper outside influences (e.g., coercion, vote-buying) can be mitigated by:
    - Permitting voters to cast multiple ballots, with each subsequent ballot replacing the previous ballot
    - Establishing that a paper ballot supersedes any Internet ballot cast by a voter
    - Ending Internet voting ahead of general voting day

Transparency and auditability:

- Oversight significantly different from traditional voting
- Nature of oversight shifts from individual ballots to the system as a whole
- Limited ability of candidates/parties/smaller jurisdictions to effectively audit Internet voting
    - May need to be outsourced
- Centralized oversight and auditing body may be necessary for local government elections (e.g., provincial government, multiple jurisdictions)
- Reviews and audits are no guarantee that a system works as promised
- Encryption and individual and independent verifiability (e.g. end-to-end verification) are important aspects of ensuring transparency and auditability

Trust:

- High level of trust in B.C. local government and provincial elections
- Internet voting will not have same level of trust as existing voting processes
- Election administrators' ability to satisfy other challenges can affect level of stakeholder trust
- Take all reasonable efforts to build as high a level of trust with stakeholders as possible; this is done by developing a system that is trustworthy

Stakeholder management:

- Vendors may underestimate significance of election administration delegating oversight
- Vendor capacity to manage large number of new clients questionable
- In-house technical expertise low in smaller local governments
    - More difficult to maintain control over vendor
    - May need assistance from provincial government or other jurisdictions
- Centralized voting administration by Elections BC for provincial elections has implications for relationship with candidates and political parties

Cost (see also Cost savings of administering Internet voting over in-person voting on page 41):

- Costs to implement not consistently defined or reported
    - Difficult to fully assess the costs of Internet voting
    - Numerous costs in addition to vendor contract/system development (e.g., system review, audit, voter education)
    - Affordability for smaller local governments questionable

7.0 EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS

A number of jurisdictions around the world have implemented Internet voting and many more have investigated it. The panel examined some of these jurisdictions and took the following lessons from those experiences. More information about the experiences of jurisdictions that have considered Internet voting, and either implemented or rejected it, is included in Appendix F.

7.1 Lessons learned for B.C.

- Internet voting is not a panacea for voter turnout (Markham)
- The more complex the process for acquiring authentication credentials, the less likely voters will be to use it (Markham, USA)
- Any pilot project must be adequately planned, tested, implemented and evaluated using predetermined criteria (UK)
- Rushing implementation results in insufficient testing and review and significantly increases the likelihood of issues that will not be identified or resolved in time (New South Wales)
- The process in use must be trusted as secure as there is no significant potential for a meaningful recount (Halifax, Estonia)
- Internet voting does not lead to increased turnout by youth (Markham, Norway)
- Allowing voters to cast a ballot multiple times (while counting only the last ballot) is an effective way to reduce the likelihood of coercion in remote voting (Estonia, Norway)
- A post-election audit by a third party should always be conducted to determine whether the integrity of the election may have been compromised and to identify opportunities for improvement (Norway, New South Wales)
- Even in jurisdictions where Internet voting is widely accepted, it still only accounts for 1/5 to 1/3 of all votes cast (Markham, Estonia)
- Jurisdictions often limit use of Internet voting to a smaller subset of the population to mitigate risk (Geneva, New South Wales)
- Most jurisdictions only offer Internet voting during advance voting periods and only allow paper ballots on general voting day (Markham, Halifax, Estonia, Norway)
- Public education and outreach ahead of an election that uses Internet voting can significantly contribute to public acceptance of Internet voting, and perhaps have an effect on voter turnout (Truro)
- Most jurisdictions claim voter convenience as a primary reason for implementing Internet voting, but many still hope it will have a positive impact on voter turnout, despite the lack of evidence (Markham, Halifax, Truro, Estonia, Geneva)

- Concerns of security and cost are most frequently given as reasons why Internet voting should not be introduced (Kitchener, Edmonton, Ontario, Canada, USA)
- Public confidence in related electoral matters (e.g., voting technology generally, electoral administration) can strongly influence the perception of Internet voting (Netherlands, Canada)

8.0 RECOMMENDATIONS

1. **Do not implement universal Internet voting for either local government or provincial government elections at this time. However if Internet voting is implemented, it should be limited to those with specific accessibility challenges. If Internet voting is implemented on a limited basis, jurisdictions need to recognize that the risks to the accuracy of the voting results remain substantial.**

   The risks of implementing Internet voting in British Columbia outweigh the benefits at this time. Therefore it is premature to implement Internet voting on a universal basis.

   Because of the strengths of Internet voting to provide increased accessibility for certain segments of the population (e.g., remote voters, voters with disabilities and voters who would otherwise need assistance to vote), Internet voting could be used in the future on a limited basis to improve access to the ballot for these groups.

   There are significant risks to implementing Internet voting that can jeopardize the integrity of an election, no matter the extent of implementation. If Internet voting is to be used in British Columbia in the future, the following three recommendations must be adhered to, including all of the principles outlined in recommendation #4.

2. **Take a province-wide coordinated approach to Internet voting.**

   If Internet voting is to be implemented at either the local government or provincial government level, election administrators should work with each other and with the provincial government to conduct a more rigorous review of the options, establish a common framework for implementation and retain control and oversight over election administration during implementation.

3. **Establish an independent technical committee to evaluate Internet voting systems and support jurisdictions that wish to implement approved systems.**

   Provincial and local government election administrators do not have the necessary technical expertise in-house to properly evaluate, verify and test high security systems such as Internet voting systems. A technical committee independent from vendors, political parties, and elected representatives, and made up of election administrators and recognized experts in Internet voting, cryptography, and computer security should be established to support the province-wide coordinated approach. The technical committee would be established by, and would report to, the B.C. Chief Electoral Officer. Such a reporting structure would emphasize the technical committee's independence. Such a committee would have to stay abreast of changes in available and emerging technology in order to establish standards and requirements that would have to be met by any Internet voting system to be

used in British Columbia. The committee would also be responsible for overseeing a rigorous review of any system being considered for use against those standards and requirements to ensure high security. Only Internet voting systems approved by the technical committee should be authorized for use in B.C. jurisdictions. The technical committee would also be responsible for monitoring the security of the systems while in use and conducting a full audit and evaluation afterwards. The work of the technical committee should be made public to ensure transparency and to build trust in any system implemented.

4. Evaluate any Internet voting system against the principles established by the panel.

While acknowledging that there will be unique factors to consider in each jurisdiction, the panel recognizes the benefit of establishing a common, or at least similar, set of principles that can be used by multiple jurisdictions in Canada to evaluate Internet voting. There is a growing consensus among election administrators of what these principles are. The panel used the eight principles established by Elections Ontario in its Alternative Voting Technologies Report[64] as a starting point from which to develop principles for British Columbia. Many of the principles outlined below share common elements with Elections Ontario's principles, but some have been amended to reflect a B.C. context or for consistency with the language used in this report. These principles must be met in addition to any standards a technical committee would establish.

Accessibility

The Internet voting process must be readily available to, and usable by, all voters eligible to vote by Internet voting, even in the presence of Internet voting-specific threats.

Ballot anonymity

The voting process must prevent at any stage of the election the ability to connect a voter and the ballots cast by the voter.

Individual and independent verifiability

The voting process will provide for the voter to verify that their vote has been counted as cast, and for the tally to be verified by the election administration, political parties and candidate representatives.

Non-reliance on trustworthiness of the voter's device(s)

The security of the Internet voting system and the secrecy of the ballot should not depend on the trustworthiness of the voter's device(s).

64 Reference #292

One vote per voter

Only one vote per voter is counted for obtaining the election results. This will be fulfilled even in the case where the voter is allowed to cast their vote on multiple occasions (in some systems, people can cast their vote multiple times, with only the last one being counted).

Only count votes from eligible voters

The electoral process shall ensure that the votes used in the counting process are the ones cast by eligible voters.

Process validation and transparency

The procedures, technology, source code, design and implementation details, and documentation of the system must be available in their entirety for free and unconstrained evaluation by anyone for testing and review for an appropriate length of time before, during and after the system is to be used. Policies and procedures must be in place to respond to issues that arise. Appropriate oversight and transparency are key to ensuring the integrity of the voting process and facilitating stakeholder trust.

Service availability

The election process and any of its critical components (e.g., voters list information, cast votes, voting channel, etc.) will be available as required to voters, election administrators, observers or any others involved in the process. If Internet voting should become unavailable or compromised, alternative voting opportunities should be available.

Voter authentication and authorization

The electoral process will ensure that before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, and that the voter is eligible to vote.

APPENDIX A - CONVENING THE PANEL

BRITISH COLUMBIA

AUG 0 7 2012

Dr. Keith Archer
Chief Electoral Officer for British Columbia
BC Elections
PO Box 9275 Stn Prov Govt
Victoria BC V8W 9J6

Dear Dr. Archer:

As you may be aware, the Premier has made a commitment to request that your office convene a non-partisan expert panel to review best practices with respect to Internet voting in other jurisdictions and to examine the issues associated with implementing Internet voting in British Columbia. I am writing to you now, as the minister responsible for the *Election Act,* to formally make that request.

As you also may be aware, several local governments in British Columbia have expressed a strong interest in offering Internet voting as well. Accordingly, should you be amenable, I would ask that the panel examine Internet voting in both local and provincial contexts, as certain factors may be unique to each level of government.

Your predecessor published a helpful in-house discussion paper on the subject last August that briefly reviewed Internet voting in other jurisdictions and examined a number of issues such as security and transparency. I am sure that paper will be useful to the panel, although of course the panel should be free to draw on research and analysis as it sees fit.

If you are amenable to undertaking this task, my ministry would be happy to assist in whatever ways you feel are appropriate.

.../2

Ministry of Justice

Office of the Minister of Justice and Attorney General

Mailing Address:
PO Box 9044 Stn Prov Govt
Victoria BC V8W 9E2
e-mail: JAG.Minister@gov.bc.ca
website: www.gov.bc.ca/justice

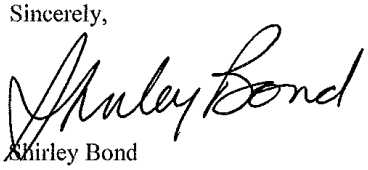
Telephone: 250 387-1866
Facsimile: 250 387-6411

Dr. Keith Archer
Page 2

I appreciate that there would be costs involved in undertaking this project. Accordingly, I am copying Mr. Douglas Horne, MLA for Coquitlam-Burke Mountain and the Chair of the Select Standing Committee on Finance and Government Services, so he is aware that you may be submitting a specific request for funding to the Committee beyond that contained in your annual budget proposal.

I look forward to a reply at your earliest convenience.

Sincerely,



Shirley Bond
Minister of Justice
and Attorney General

pc: The Honourable Ida Chong
Mr. Douglas Horne, MLA
Mr. Leonard Krog, MLA

ELECTIONS BC
A non-partisan Office of the Legislature

Mailing Address:
PO Box 9275 Stn Prov Govt
Victoria BC V8W 9J6

Phone: 250-387-5305
Toll-free: 1-800-661-8683/ TTY 1-888-456-5448
Fax: 250-387-3578
Toll-free Fax: 1-866-466-0665
Email: electionsbc@elections.bc.ca
Website: www.elections.bc.ca

August 9, 2012

Honourable Shirley Bond
Attorney General
Ministry of Justice
PO Box 9044 Stn Prov Govt
Victoria, BC V8W 9E2

Honourable Shirley Bond:

Thank you for the invitation to convene and chair a panel that will enquire into prospects for Internet voting in British Columbia.

As an Independent Officer of the Legislative Assembly, I am very pleased to convene and chair a panel for this purpose. I am writing to advise you, as well as those copied on this letter, how I intend to proceed.

Mandate and Authority
Convening a panel to research and draft recommendations to the Legislative Assembly on Internet voting is authorized pursuant to section 12(2)(a) of the *Election Act*.

Scope
Following and extending the Elections BC report entitled, *Discussion Paper: Internet Voting*, the panel will examine opportunities and challenges related to the potential implementation of Internet-based voting for provincial or local government elections in British Columbia.

Reporting
The method for gathering input and feedback from experts and the public will be determined by the panel. Additionally, the panel, when established, will develop a work plan and the timeline for reporting.

Composition
I will chair the panel and will invite four additional members. Members will be drawn from a wide spectrum reflecting expertise in technology, cryptography, Internet security policy, and electoral administration. All members will have a high level of independence and judgment.

Secretariat
The secretariat function of the panel will be provided by Elections BC.

...2/

Budget
The costs of the panel are estimated to be $420,000. I expect the majority of these costs to be incurred in the current fiscal year, and I will ask the Select Standing Committee on Finance and Government Services to recommend my office be granted access to the Contingencies Vote for 2012/13. Any necessary funding for next fiscal year will be requested as part of Elections BC's annual budget proposal for 2013/2014.

If you, or those copied on this letter, have comments on any aspect of the panel as outlined, please communicate these by August 23, 2012. My intention is to write to the Select Standing Committee on Finance and Government Services the following week to request funding for the panel. I intend to select the panel by September 7 and to convene the first meeting by October 1.

Sincerely,

Keith Archer, Ph.D.
Chief Electoral Officer
British Columbia

c. Honourable Bill Barisoff, MLA
Speaker of the Legislative Assembly

Craig James
Clerk of the Legislative Assembly

Douglas Horne, MLA
Chair, Select Standing Committee on Finance and Government Services

Leonard Krog, MLA
Critic for Attorney General

Honourable Rich Coleman, MLA
Government House Leader

John Horgan, MLA
Opposition House Leader

Honourable Ida Chong, MLA
Minister of Community, Sport and Cultural Development

APPENDIX B - PANEL MEMBERS

KEITH ARCHER, Ph.D.

Keith Archer became British Columbia's Chief Electoral Officer on September 1, 2011. He brings over thirty years of experience in electoral administration research and education to the position of Chief Electoral Officer.

Prior to his appointment, Keith Archer was Professor of Political Science at the University of Calgary (1984) and Director of Research at the Banff Centre. He completed BA and MA degrees in Political Science at the University of Windsor, and a Ph.D. at Duke University. His teaching and research has focused on the study of elections and voting. He is the author, co-author or co-editor of seven books and over thirty articles and chapters in the area.

Keith Archer's experience and expertise has contributed to a number of projects including the Administration and Cost of Elections project (a collaborative initiative of the United Nations, the International Institute for Democracy and Electoral Assistance (IDEA) and the International Foundation for Election Systems, among others), the Royal Commission on Electoral Reform and Party Financing in Canada (The Lortie Commission), Bill C-16 (Expanded Voting Opportunities) and he has provided expert opinion involving the Canadian Charter of Rights and Freedoms on the section 3 "right to vote."

DR. KONSTANTIN (KOSTA) BEZNOSOV

Konstantin (Kosta) Beznosov is an Associate Professor at the Department of Electrical and Computer Engineering, University of British Columbia (UBC), Vancouver, where he founded and directs the Laboratory for Education and Research in Secure Systems Engineering (LERSSE). His primary research interests are distributed systems security, usable security, secure software engineering, and access control. Prior UBC, Dr. Beznosov was a Security Architect with Quadrasis, Hitachi Computer Products (America), Inc, where he designed and developed products for security integration of enterprise applications, as well as consulted large telecommunication and banking companies on the architecture of security solutions for distributed enterprise applications. Dr. Beznosov did his Ph.D. research on engineering access control for distributed enterprise applications at the Florida International University. He actively participated in standardization of security-related specifications (CORBA Security, RAD, SDMM) at the Object Management Group, and served as a co-chair of the OMG's Security SIG. Having published a number of research papers on security engineering in distributed systems, he is a co-author of "Enterprise Security with EJB and CORBA" and "Mastering Web Services Security." He has served on program committees and/or helped to organize SOUPS, CCS, NSPW, NDSS, ACSAC, SACMAT, CHIMIT. Prof. Beznosov is an associate editor of ACM Transactions on Information and System Security (TISSEC) and International Journal of Secure Software Engineering (IJSSE).

LEE-ANN CRANE

Lee-Ann Crane has been employed with the Regional District of East Kootenay since 1979 and has been the Chief Administrative Officer since 1998.

Lee-Ann has served in various capacities on the Board of the Local Government Management Association of BC. She is currently Chair of their Elections Committee and was instrumental in the development and publication of the Local Government Elections Manual, and continues to be responsible for content and editing. Lee-Ann also serves as a resource to local government election officials throughout B.C. and participates in review of local election legislative changes.

DR. VALERIE KING

Valerie King is Professor of Computer Science at the University of Victoria and has been a faculty member there since 1992. She received an A.B. degree in Mathematics from Princeton University and a Ph.D. in Computer Science and a J.D., both from the University of California at Berkeley. She was a post-doctoral fellow at the University of Toronto and Princeton University, a Research Scientist at NECI, Compaq SRC and HP Labs, a Visiting Researcher at Microsoft Research SVC and at the Simons Institute for Theory of Computing in Berkeley, and a Visiting Professor at the University of Copenhagen and Hebrew University. She is currently a member of the Institute for Advanced Study in Princeton.

Dr. King's current research concerns randomized algorithms, data structures, and distributed computing, with applications to networks and security. She has served on numerous technical committees and panels, including panels for the Natural Sciences and Engineering Research Council of Canada and the U.S. National Science Foundation, and has published over sixty scholarly papers and book chapters. She is a member of the Association for Computing Machinery and the State Bar of California.

GEORGE MORFITT, FCA

George Morfitt is a graduate of the University of British Columbia and a Chartered Accountant. After a 20-year career as Chief Financial Officer in the private sector in Vancouver, he served two terms as Auditor General of British Columbia. Mr. Morfitt has held senior executive positions in a number of organizations, including: President, BC Institute of Chartered Accountants; Chair, Universities Council of BC; and Chair, UBC Board of Governors. He is a former alderman for the municipality of West Vancouver and is a past President of the Canadian Squash Racquets Association.

Mr. Morfitt is a Fellow of the BC Institute of Chartered Accountants and a Queen's Diamond Jubilee medalist. He currently serves as Chair of WorkSafeBC and is a past director of the Motor Vehicle Sales Authority of BC, the BC Safety Authority and the Health Council of Canada. Mr. Morfitt is an inducted member of the BC Sports Hall of Fame and is past Chair of Canadian Sport Centre Pacific.

APPENDIX C - EXPERT PRESENTERS

Presentations

Ian Bailey (Executive Director, Architecture and Standards and Information Security, Ministry of Technology, Innovation and Citizens' Services)

Kevena Bamford (Executive Director, Provincial Identity Management Program, Ministry of Technology, Innovation and Citizens' Services)

Anton Boegman (Deputy Chief Electoral Officer – Electoral Operations, Elections BC)

Michelle Dann (Ministry of Community, Sport and Cultural Development)

Ben Goldsmith (Senior Electoral Advisor, International Foundations for Electoral Systems)

Dr. J. Alex Halderman (Assistant Professor of Electrical Engineering and Computer Science, University of Michigan)

Bette-Jo Hughes (Associate Deputy Minister of Technology, Innovation and Citizens' Services & Acting Chief Information Officer)

Stephen Huycke (Acting Deputy Clerk, City of Markham)

Denise McGeachy (Ministry of Community, Sport and Cultural Development)

Susan McMurray (Manager of Research and Policy, Elections Ontario)

Cathy Mellett (Chief Clerk, Halifax Regional Municipality)

Stefan Morales (Ministry of Community, Sport and Cultural Development)

Dr. Ronald L. Rivest (Professor of Computer Science, Massachusetts Institute of Technology)

Dr. Melanie Volkamer (Assistant Professor, Technische Universität Darmstadt)

Lorie Wells (Deputy Chief Electoral Officer, Elections Ontario)

Internet Voting Technology Vendors

Everyone Counts Canada Inc.

Intelivote Systems Inc.

Scytl Canada Inc.

APPENDIX D - QUESTIONS TO INTERNET VOTING VENDORS

1. Must an Internet voting solution require voters to assume responsibility for ensuring their computers are free from malware that could compromise the secrecy of the ballot or prevent their ballot from being cast in the way in which they intend? How does your solution mitigate this risk?

2. With what level of confidence can an election administrator trust that the individual who has cast a ballot using an Internet voting solution is the individual to whom the election administrator believes they have provided the ballot?

3. How would you respond to the following statement:

   > Recent cyber attacks on major organizations such as financial institutions, the U.S. Department of Defense, the FBI and Google have proven that networks cannot be secured against a well-funded coordinated attack and therefore any vendor claiming to provide a secure Internet voting solution is misleading you.

4. When using an Internet voting solution, how can election administrators, political parties, candidates and voters trust that all votes were cast and counted as intended?

5. How much technical expertise must election administrators have within their organization to provide a reasonable level of oversight to a vendor providing an Internet voting solution?

6. To what extent is your application code proprietary? Can it be made available for scrutiny by others, and under what conditions?

7. How can it be proven that the version of application code that has been tested and reviewed is indeed the version that is running during the election?

8. How can political parties and candidates scrutinize an Internet voting solution? Must they delegate this right to a third party (e.g., an independent audit firm)? Can individual political parties or candidates appoint their own scrutineers or must they all trust a single third party appointed by the election administrator?

9. Local government elections in B.C. are administered separately by each jurisdiction, but under a common legislative framework with a common election period. How many simultaneous elections can a single vendor reasonably support? ("support" includes both technical and contract management capabilities)

10. With regard to registration/eligibility for Internet voting and the provision of authentication credentials, how can an Internet voting solution vendor balance the expectations of voters for a simple process with the expectations of election administrators for a secure process?

11. Some jurisdictions distribute elements of Internet voting amongst multiple vendors in order to reduce risk by avoiding relying on a single vendor. How would you recommend an Internet voting solution be divided?

12. Internet voting standards are emerging from various international bodies. Do you evaluate your Internet voting solution against any particular standard(s)? If so, which body's standards are you using and how does your solution meet the standard?

APPENDIX E - REFERENCE LIST

The following resources have been directly referenced in this report. A full bibliography is available on the Independent Panel on Internet Voting website (internetvotingpanel.ca).

7. European Commission for Democracy Through Law (Venice Commission). (July 2002). Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report. Venice, Italy: Council of Europe.

27. Office for Democratic Institutions and Human Rights. (2005). Election Observation Handbook, Fifth Edition. Warsaw, Poland: OSCE/ODIHR.

38. U.S. Election Assistance Commission. (2011, September 14). Testing and Certification Technical Paper #2: A Survey of Internet Voting. Washington, D.C.

45. Beroggi, G. (2007) E-Voting through the Internet and with Mobile Phones. United Nations Public Administration Network.

48. Goodman, N., Pammett, J. H., & DeBardeleben, J. (2010, February). A Comparative Assessment of Electronic Voting. Ottawa, Canada.

57. Department of Defense. (2001, June). Voting Over the Internet Pilot Project Assessment Report. Prepared by the Federal Voting Assistance Program (FVAP). Washington, D.C.

60. The Electoral Commission. (2002, August). Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes. London, United Kingdom.

62. The Electoral Commission. (2007, August). Key Issues and Conclusions: May 2007 Electoral Pilot Schemes. London, United Kingdom.

71. Kim, H. (2005, June 23). Risk Analysis of Traditional, Internet, and Other Types of Voting Alternatives for Town of Markham. Markham, Ontario.

75. McKinstry, J. (2010, January 26). Peterborough's Experience with Internet Voting. Presented at Policy Workshop – Internet Voting: What can Canada Learn? at Carleton University, Ottawa, Canada.

76. Mellett, C. (2010, January). HRM's Experience with Electronic Voting. Presented at Policy Workshop – Internet Voting: What can Canada Learn? at Carleton University, Ottawa, Canada.

83. Ministry of Local Government and Regional Development. (2006). Electronic voting – Challenges and Opportunities. Oslo, Norway.

84. Ministry of Local Government and Regional Development. (2011) Summary of the ISF Report. Retrieved on June 20, 2012, from http://www.regjeringen.no/nb/dep/krd/prosjekter/e-vote-2011-project/evaluering/evaluations-of-the-e-voting-trials/evaluations-of-the-e-voting-trials-in-201/summary -of-the-isf-report.htm?id=685824

94. Hastings, N., Peralta, R., Popoveniuc, S., & Regenscheid, A. (2011, February). Security Considerations for Remote Electronic UOCAVA Voting. Gaithersburg, Maryland: National Institute of Standards and Technology.

95. Regenscheid, A. & Hastings, N. (2008, December). Threat Analysis on UOCAVA Voting Systems. Gaithersburg, Maryland: National Institute of Standards and Technology.

99. New South Wales Electoral Commission. (2011, June). Technology Assisted Voting Audit: Post-Implementation Report. Sydney, Australia.

102. Office for Democratic Institutions and Human Rights. (2007, March 12) OSCE / ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006. Vienna, Austria.

109. State Chancellery. (2007, July). State Council's Report to the Grand Council on the Geneva Electronic Voting Project. Geneva, Switzerland.

118. U.S. Election Assistance Commission. (2011, April 6). Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes. Washington D.C.

120. Tennant, N. E. (2011, January 19). West Virginia Uniformed Services and Overseas Citizens: Online Voting Pilot Project. Charleston, West Virginia.

121. Elections BC. (2011, August). Discussion Paper: Internet Voting. Victoria, Canada: Elections BC.

123. Elections Ontario. (2011, November 15). Request For Proposal for the Provision of Network Voting System Internet and Telephone Pilot Project. Toronto, Canada: Elections Ontario.

130. International Idea. (2011, December). Introducing Electronic Voting: Essential Considerations. Stockholm, Sweden: International IDEA.

131. Goldsmith, B. (2011, May). Electronic Voting and Counting Technologies: A Guide to Conducting Feasibility Studies. Washington, D.C.: International Foundation for Electoral Systems.

132. Elections Ontario (2011). Network Voting System Internet and Telephone Pilot Project Description. Toronto, Canada: Elections Ontario.

135. Elections Canada. (2011, April 1). I-Voting Pilot Project Progress Report. Ottawa, Canada: Elections Canada.

136. Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009, June 26). Internet Voting in Comparative Perspective: The Case of Estonia. PS: Political Science and Politics, 42, 497-505.

139. Working Group on Digital Identity and Authentication. (2011, April 26). Detailed Use Cases for Digital Identity. British Columbia, Canada: Office of the Chief Information Officer.

140. Esteve, J. B. & Goldsmith, B. (2012, June). Compliance With International Standards: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

141. Esteve, J. B., Goldsmith, B., & Turner, J. (2012, June). Speed and Efficiency of the Vote Counting Process: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

142. Esteve, J. B., Goldsmith, B., & Turner, J. (2012, June). International Experience with E-Voting: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

144. Nevo, S. & Kim, H. (2006). How to Compare and Analyze Risks of Internet Voting Versus Other Modes of Voting. E-Government: An International Journal, 3 (1), 105-112.

145. Kim, H. (2010, March 23). A Study of Internet Voting Security Risks and Accessibility Opportunities for the Town of Markham. Toronto, Canada.

146. Goodman, N., Pammett, J., & Debardeleben, J. (2010, Autumn). Internet Voting: The Canadian Municipal Experience. Canadian Parliamentary Review, 33(3), 13-21.

148. Ansper, A., Heiberg, S., Lipmaa, H., Overland, T. A., & van Laenen, F. (2011). Security and Trust for the Norwegian E-voting Pilot Project. Oslo, Norway: Ministry of Local Government and Regional Development.

150. Beaucamps, P., Reynaud-Plantey, D., Marion, J.-Y., & Filiol, E. (2009). On the use of Internet Voting on Compromised Computers. Rennes, France: Equipe Carte-Loria and Army Signals Academy Virology and Cryptology Laboratory.

152. Bochsler, D. (2010, May 26). Can Internet voting increase political participation? Remote electronic voting and turnout in Estonian 2007 parliamentary elections. Central European University, Budapest: Centre for the Study of Imperfections in Democracies.

154. Chowdhury, M. J. M. (2010). Comparison of e-voting schemes: Estonian and Norwegian solutions. University of Tartu, Estonia.

156. Election Process Advisory Commission. (2007, September 27). Voting with Confidence. The Hague: Ministry of Interior and Kingdom Relations.

157. Science and Technology Options Assessment. (2011, March 23) Can E-Voting Increase Electoral Participation? European Parliament.

164. Joint Standing Committee on Electoral Matters. (2009, March). Report of the 2007 Federal Election Electronic Voting Trials. Parliament of Australia. Canberra, Australia.

166. Kripp, M. (2011, March 11). Internet Voting in Estonia – Necessary to Maintain Turnout and Integrate Voters. Retrieved July 24, 2012 from http://www.e-voting.cc/en/internet-voting-in-estonia-necessary-to-maintain-turnout-and-integrate-voters-archive-032011

167. Nestas, L. H. (2010, June). Building Trust in Remote Internet Voting (Master's thesis). University of Bergen, Norway.

173. Puiggali, J. & Castello, S. G. (2012). Cast-as-Intended Verification in Norway. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

174. Puiggali, J. & Castello, S. G. (2012). Cast-as-Intended Verification in Norway. Presentation at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

176. Driza-Maurer, A., Spycher, O., Taglioni, G., & Weber, A. (2012). E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

180. Budurushi, J., Neumann, S., & Volkamer, M. (2012). Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

184. Stenerud, I. S. G. & BULL, C. (2012). When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

187. Beckert, B., Lindner, R., Goos, K., Hennen, L., Aichholzer, G., & Strauβ, S. (2011, November). E-public, E-participation and E-voting in Europe - Prospects and Challenges. Brussels, Belgium: European Parliament.

190. Krimmer, R. & Volkamer, M. (2006). Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting. Paper presented at the EVOTE 2006 conference, Lochau/Bregenz, Austria.

191. Office for Democratic Institutions and Human Rights. (2012, January 30). Swiss Confederation Federal Assembly Elections, October 23, 2011: OSCE/ODIHR Election Assessment Mission Report . Warsaw., Poland: OSCE/ODIHR.

192. Chevallier, M. (2003). Internet Voting: Status, Perspectives and Issues. Presentation to ITU E-Government workshop, Geneva, Switzerland.

194. State Chancellery. (n.d.) Discover the Video [Video file]. Canton of Geneva. Retrieved September 24, 2012, from http://www.geneve.ch/evoting/english/welcome.asp

195. State Chancellery. (2013). The Geneva Internet Voting System. Geneva, Switzerland: Imprimerie genevoise SA.

197. State Chancellery. (2009, September). History and Results of the Tests and Official Ballots. Retrieved 13 August, 2013, from http://www.geneve.ch/evoting/english/historique.asp

203. Regenscheid, A. & Beier, G. (2011, September). Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. Gaithersburg, Maryland: National Institute of Standards and Technology.

204. E-Voting Working Group. (2012). Record of Discussion, May 3-4, 2012. Canada.

205. Capital Region Partnership. (2012, February 1). Internet Voting Pilot Proposal for 2013 Municipal Election. Edmonton, Canada.

206. Clark, J. (2011). Democracy Enhancing Technologies: Toward Deployable and Incoercible E2E Elections (Doctoral dissertation). University of Waterloo, Canada.

207. Delvinia. (2004). Internet Voting and Canadian e-Democracy in Practice: The Delvinia Report on Internet Voting in the 2003 Town of Markham Municipal Election. Markham, Canada.

208. Delvinia. (2011). eDemocracy and Citizen Engagement: The Delvinia Report on Internet Voting in the Town of Markham. Markham, Canada.

210. Elections Ontario. (2012, October). Network Voting Research Summary. Toronto, Canada: Elections Ontario.

211. Elections Ontario. (2012). Network Voting Business Case. Toronto, Canada: Elections Ontario.

213. Clark, J. (2012, November). Security Risks Related to Internet Voting. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

214. Goodman, N. (2012) An Assessment of Internet Voting in Canada. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

215. Goodman, N. (2012, November). Issues Guide: Internet Voting. Edmonton, Canada: University of Alberta.

216. Pammett, J. (2012, November). Internet Voting in Comparative Perspective: Context and Issues. Presentation to Citizens' Jury on Internet Voting. Edmonton, Canada.

217. Delvinia. (2012). Internet Voting In Markham. Presentation to Citizens' Jury on Internet Voting, Edmonton, AB.

218. Scytl. (2012) Security of the Internet Voting Trial: Security Components. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

223. New South Wales Electoral Commission. (2011, December 9). NSW State General Election and Clarence By-election iVote presentation. Sydney, Australia.

224. Gosse, R. (2012, November 2). Staff Report on Internet Voting to Finance and Corporate Services Committee. Kitchener, Canada.

226. Office of the City Clerk. (2013, February 6). City of Edmonton Internet Voting. Presentation to City Council, Edmonton, Canada.

227. Huycke, S. & Tecsa, T. (2012, September 28). City of Markham Online Voting Experience. Presentation to the Union of British Columbia Municipalities - 2012 Annual Convention, Victoria, Canada.

228. Habkirk, A. (2012, September 27). Voter Turnout: 2011 B.C. Local Government Elections. Presentation to Union of British Columbia Municipalities, Victoria, Canada.

231. Coleman, S. (2005). Just How Risky Is Online Voting? Information Polity, 10, 95-104.

233. Town of Truro. (2012, September). Voter Newsletter: Your guide to Elections 2012. The Town of Truro, Canada.

235. Council of Europe (2011, February 16). Guidelines on Transparency of e-Enabled Elections. Strasbourg, France.

236. Halifax Regional Municipality By-Law A-400 Respecting Alternative Voting. (2008). Halifax, Canada.

238. Billett, J. (2012, December 10). Finance and Corporate Services Committee (Meeting minutes). City Kitchener, Canada.

240. Cybernetica AS. (n.d.) Internet voting solution [Brochure]. Tallinn, Estonia.

241. Elections Canada. (2008, February). Strategic Plan, 2008-2013. Ottawa, Canada: Elections Canada.

242. Barette, P. (2013, February) Interest of Canadians in Internet Voting (2004, 2006, 2008 and 2011) (Research Note). Ottawa, Canada: Elections Canada.

244. Elections BC. (2013). 2013 Elections BC Post-election Voter/Non-Voter Satisfaction Survey. Victoria, Canada: Elections BC.

246. National Post Staff. (2012, March 27). Cyber attack on NDP leadership vote involved more than 10,000 computers. National Post. Retrieved from http://www.nationalpost.com

247. Perlroth, N., & Sanger, D. (2013, July 13). Nations Buying as Hackers Sell Flaws in Computer Code. New York Times. Retrieved from http://www.nytimes.com

248. Davis, S. & Kennedy, L. (2011, December 14) Potential use of Remote Electronic Voting Options: Internet Voting. Edmonton, Canada.

249. Seccuris. (2012, December 10). Executive Summary: Business and Technical Threat Risk Assessment for Electronic Voting.

250. Whittaker, P. (2012, October 19). Letter to Capital Regional City Managers re: Joint Internet Voting Pilot. Alberta, Canada; Government of Alberta Ministry of Municipal Affairs.

251. City of Edmonton. (2013). Internet Voting. Retrieved July 19, 2013, from http://www.edmonton.ca/city_government/municipal_elections/internet-voting.aspx

252. Rodrigues, A. (2013, February 6). Edmonton City Council Shelves Online Voting Idea. Edmonton Sun. Retrieved from http://www.edmontonsun.com

253. MacKinnon, L. (2013, April 30). Elections Canada Drops Plan For Online Voting Due to Cuts. CBC News. Retrieved July 19, 2013, from http://www.cbc.ca

254. ERR News. (2013, July 12). E-Voting Source Code Made Public. Retrieved July 22, 2013, from http://news.err.ee/politics/0233b688-b116-44c3-98ca-89a4057acad8

255. Centre for Public Involvement. (2012, November). Citizens Jury on Internet Voting Expert Witness Information Package. Edmonton, Canada.

256. Elections BC. (2013, June 23) Voting Results Change History Report, Saanich North and the Islands, 40th Provincial General Election. Victoria, Canada: Elections BC.

257. Estonian National Electoral Committee. Statistics about Internet Voting in Estonia. Retrieved July 23, 2013, from http://vvk.ee/voting-methods-in-estonia/engindex/statistics

258. Office of the Chief Information Officer. (2013, June 18). BC Services Card: The Possibilities. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

260. Lychkovakh, O. (2012, March). Success Case: Norway Local Government Elections. Scytl.

261. State Chancellery. (2013). List of all eEnabled official ballots conducted in Geneva since the start of the Internet voting project. Geneva, Switzerland.

263. Neufeld, H. (2013, March). Compliance Review: Final Report and Recommendations. Ottawa, Canada.

264. Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004, January 21). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). United States.

265. Department of Defense. (2007, May). Department of Defense: Expanding the Use of Electronic Voting Technology for UOCAVA Citizens. Washington, D.C.

266. Jefferson, D., Rubin, A. D., & Simons, B. (2007, June). A Comment on the May 2007 DOD Report on Voting Technologies for UOCAVA Citizens. United States.

267. Schwartz, J. (2004, January 21). Report Says Internet Voting System Is Too Insecure to Use. New York Times. Retrieved from http://www.nytimes.com

268. National Association of Secretaries of State. (2009, November). NASS Summary of the Military and Overseas Voter Empowerment Act (MOVE Act).

269. West Virginia Secretary of State. (2012, September 13). Tennant: West Virginia's Military, Veterans, and Overseas Citizens Have Several Convenient Voting Options. Retrieved on August 13, 2013, from http://www.sos.wv.gov/news/topics/elections-candidates/Pages/TennantWestVirginiasMilitaryVeteransandOverseas.aspx

270. West Virginia Secretary of State. (2010, May 21). West Virginia's Internet Voting Pilot Program Featured In Pew Center Newsletter. Charleston, West Virginia. Retrieved on August 13, 2013, from http://www.sos.wv.gov/news/topics/elections-candidates/Pages/WestVirginia'sInternetVotingPilotProgramFeaturedInPewCenterNewsletter.aspx

271. Moretti, M. (2010, May 20). Internet voting for military, overseas voters debuts in West Virginia - Clerks and secretary of state pleased with first use. Electionline Weekly.

272. Collins, B. (2012, May 18). NIST Activities on UOCAVA Voting. Gaithersburg, Maryland: National Institute of Standards and Technology.

273. Ministry of Local Government and Regional Development. (2012, December 17). Internet voting pilots announced for 2013 [Press release]. Retrieved from http://www.regjeringen.no/en/dep/krd/press/press-releases/2012/new-pilot-with-internet-voting-in-2013.html?id=710138

274. Joye, C., Smith, P., & Kerin, J. (2013, July 27). Spy Agencies Ban Lenovo PCs on Security Concerns. Australian Financial Review. Retrieved from http://www.afr.com/

275. Vassil, K. & Weber, T. (2009, September). A Bottleneck Model of E-voting: Why Technology Fails to Boost Turnout. Paper presented at the Annual Meeting of the American Political Science Association, Toronto, Canada.

276. Trechsel, A. & Vassil, K. (2010, January). Internet Voting In Estonia: A Comparative Analysis of Four Elections since 2005. Florence, Italy: European University Institute.

278. Mellett, C. (2013, July 5). Personal communication.

279. Mellett, C. (2013, February 8). Electronic Voting 2012: Municipal and School Board Elections. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

280. Office of the e-Envoy. (2002). In the Service of Democracy: A Consultation Paper on a Policy for Electronic Democracy. London, United Kingdom.

281. Halderman, J. A. (2013, January 25). Internet Voting: What are the Security Risks? Presentation to Independent Panel on Internet Voting, Victoria, Canada.

282. Rivest, R. (2013, January 25). Is Internet Voting a Good Idea? Presentation to Independent Panel on Internet Voting, Victoria, Canada.

283. Elections BC. (2012, November 7). British Columbia's Current Voting Model. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

284. Ministry of Community, Sport and Cultural Development. (2012, December 19). Local Government Election Model in B.C. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

285. Local Government Elections Task Force. (2010, January). Backgrounder on Local Government Elections. Victoria, Canada.

286. Volkamer, M. (2013, February 9). Electronic Voting. Presentation to Independent Panel on Internet Voting, Victoria, Canada

287. Elections Ontario. (2013, February 8). Elections Ontario's Alternative Voting Technology Review. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

289. Butts, R. (2013, January 15). Review of the 2012 Municipal and School Board Elections. Information Report to Halifax Regional Municipality Council. Halifax, Canada.

290. Butts, R. (2011, September 27). 2012 Municipal and School Board Elections. Recommendations Report to Halifax Regional Municipality Council. Halifax, Canada.

291. Mellett, C. (2013, June 19, 2013). Personal communication.

292. Elections Ontario. (2013, June). Alternative Voting Technologies Report - Chief Electoral Officer's Submission to the Legislative Assembly. Toronto, Canada: Elections Ontario.

293. Huycke, S. & Tecsa, T. (2012, November 13). Markham Votes 2014 - Internet Voting Program. Presentation to Special General Committee Meeting, Markham, Canada.

294. Ernst & Young. (2012, October 23) Specified Auditing Procedures Report: Electronic Voting - Halifax Regional Municipality. Halifax, Canada.

295. Goodman, N. (2013, July 15). Personal communication.

296. Town of Truro 2012 Elections. Retrieved from http://www.facebook.com/pages/Town-of-Truro-2012-Elections/528265507199852

297. Kennedy, L. (2012, November 23). The Edmonton Jellybean Election Experience. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

304. Oostveen, A.-M. (2010, September). Outsourcing Democracy in the Netherlands: The Risk of Contracting Out E-Voting to the Private Sector. Paper presented at 'Internet, Politics, Policy 2010: An Assessment' conference, Oxford, United Kingdom.

305. Jacobs, B. & Pieters, W. (2009). Electronic Voting in the Netherlands: from early Adoption to early Abolishment. Netherlands.

306. Teague, V. & Wen, R. (n.d.) Problems with the iVote Internet Voting System. The Computing Research and Education Association of Australasia. Australia.

310. Ostvold, B. M. & Karlsen, E. K. (2012). Public Review of E-Voting Source Code: Lessons learnt from E-Vote 2011. Paper presented at the NIK-2012 conference, Bodo, Norway.

317. Letter to T.D. Rust and Virginia Joint Committee on Technology & Science. (2012, July 11).

321. New South Wales Electoral Commission. (2013, August). iVote Strategy for the NSW State General Election 2015 - Key Issues, Guidelines, Application Architecture and Voting Protocol. Sydney, Australia.

323. Mayrand M. (2012, June 24). Personal communication. Halifax, Nova Scotia.

324. Ministry of Local Government and Regional Development. (2013, September 5). Seminar on Internet Voting. Retrieved from http://www.regjeringen.no/en/dep/krd/lyd_bilde/nett-tv/seminar-on-internet-voting.html?id=735137

325. Kiniry, J., Morkan, A., Cochran, D. & Fairmichael, F. (2007). The KOA Remote Voting System: A Summary of Work To-Date. Trustworthy Global Computing, 244-262. Springer Berlin Heidelberg.

329. Ministry of Local Government and Regional Development. (2013, September 9). Decryption and Counting Ceremony of the Internet Votes, English Language. Retrieved from http://www.regjeringen.no/nb/dep/kmd/lyd_bilde/nett-tv/decryption-and-counting-ceremony-of-the-.html?id=735138

330. Ministry of Local Government and Regional Development. (2013, September 6). Protection of the Internet Votes. Retrieved from http://www.regjeringen.no/en/dep/krd/lyd_bilde/nett-tv/seminar-on-internet-voting.html?id=735137

331. Ministry of Local Government and Regional Development. (2013, September). How to Vote Via the Internet in the Parliamentary Election 2013. Retrieved from http://www.regjeringen.no/pages/597658/how_to_vote_internet.pdf

332. Brightwell, I. (2013, November 1). Personal communication. New South Wales, Australia.

333. Office for Democratic Institutions And Human Rights. (2013, December 16) OSCE/ODIHR Election Assessment Mission Final Report: Norway Parliamentary Elections 9 September 2013. Warsaw, Poland.

334. Statistics Canada. (2013, December). Canadian Survey on Disability, 2012. Ottawa, Canada.

335. Elections BC. (2013, December 18). Personal communication.

336. Elections BC. (2014, January 15). Personal communication.

337. Elections BC. (2014, January 17). Personal communication.

338. Elections BC. (2014, January 21) Statement of Votes for the 40th Provincial General Election. Victoria, Canada.

APPENDIX F - EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS

The use of Internet voting is not as widespread as some may think. Of the 11 countries to have used Internet voting for at least one binding governmental election, only jurisdictions in seven countries still do.[65] Most implementations of Internet voting are limited to local government elections or to subsets of the entire voting population (e.g., remote voters). The jurisdictions highlighted in this appendix were chosen by the panel to be the most prominent, or to have the most representative experiences with Internet voting to British Columbia (whether implemented or investigated and rejected). These summaries are examples and do not represent an exhaustive list of Canadian or global Internet voting experiences. The amount of detail provided in the summary for each jurisdiction varies, in part due to the amount of, and detail in, existing research available for those elections.

Canada - Implemented

Markham, Ontario[66]

Origins

Until the 2008 Local Government Elections in the Halifax Regional Municipality, Markham, Ontario was the largest jurisdiction in Canada to implement Internet voting. Markham conducted its first local government election using Internet voting in 2003 with a hope that it would reverse a declining level of voter turnout. While this goal was not realized, the city felt that Internet voting would prevent a further decrease in voter turnout and allow it to provide a convenient and cost effective voting opportunity. For these reasons, among others, Markham has since conducted two additional mayoral and councillor elections in 2006 and 2010 and is making preparations to include an Internet voting option for the 2014 elections. In each election Markham has only provided in-person and Internet voting opportunities – it does not permit telephone voting or voting by mail, though it is considering the feasibility of adding telephone voting in 2014 as well as increasing the number of days for Internet voting or expanding Internet voting up to and including general voting day. The city utilizes a Request for Proposals (RFP) process ahead of each election to select its Internet voting system.

Process

Registered voters in Markham must register separately in order to use Internet voting using a two-stage process. All registered voters are sent a package in the mail that contains a unique Personal Identification Number (PIN) that the voter can use along with the voter's date of birth (DOB) to log into Markham's Internet voting registration website. On the website the voter creates a personalized password and will use this password along with a new PIN sent to the voter in the mail in order to vote.

65 Reference #142
66 For more information about Markham's experience with Internet voting, see references #38, 48, 71, 142, 145, 146, 207, 208, 214, 215, 217, 227, 293

In Markham, Internet voting was offered twenty-four hours a day during the advance voting period. In 2003, the advance voting period was 5 days, and in 2006 and 2010 it was increased to 6 days. Ahead of its next election in 2014, Markham is considering the feasibility of increasing the number of days for Internet voting even further or expanding Internet voting up to and including general voting day. It is also planning to add expanded audit capabilities to both its Internet voting processes and technology.

Markham's implementation of Internet voting permitted under-votes,[67] but not over-votes.[68]

	2003	2006	2010
Population	~230,000	~260,000	~300,000
Eligible voters	158,000	164,000	164,000
Overall turnout (#)	42,198	61,948	65,927
Overall turnout (%)	28.0%	37.9%	35.5%
Internet voting registration (#)	11,708	16,251	17,231
Internet voting turnout (#)	7,210	10,639	10,597
Internet voting as % of eligible voters	4.5%	6.5%	5.7%
Internet voting as % of votes cast	17.1%	17.2%	16.1%
When offered	5 days during advance voting period; 24h/d	6 days during advance voting period; 24h/d	
Vendor	ES&S	ES&S	ES&S and Intelivote

Results

The introduction of Internet voting in Markham has not led to the increase in voter turnout once expected, but it does consider Internet voting to be a success. City staff point to its repeated use by voters and the high levels of voter satisfaction reported in post-election experience surveys. Convenience has become the primary rationale for continuing with Internet voting, though city staff also consider Internet voting to be a way to help maintain the election budget at current levels.

Analysis of the Markham voter turnout research shows that Internet voting is used primarily by middle-aged voters[69] (the age cohort that also has the highest levels of voting using traditional voting opportunities) and does not appear to lead to increased voting by younger voters.

67 Under-vote: Marking the ballot for no candidate, or fewer than the maximum number allowed in the race; where only one vote was permitted this results in the ballot being rejected; where multiple choices are permitted, the valid markings are still recorded; often this occurs on purpose to indicate a protest vote, but can also occur unintentionally

68 Over-vote: Marking the ballot for more than the maximum allowable number of candidates; this results in the ballot being rejected for that race and no vote recorded

69 66% of all Internet ballots in Markham were cast by voters aged 40-69.

While Markham has one of the longest histories with Internet voting in Canada and reports high levels of voter satisfaction with the system, Internet voting still only makes up approximately 16% of all votes cast in the election. Furthermore, the number of Internet ballots cast in 2010 did not change significantly from 2006 despite an increase of almost 4,000 votes overall from one election to the next.

Halifax, Nova Scotia[70]

Origins

At the request of the council, Halifax Regional Municipality (HRM) staff first began to examine alternative voting methods in 2004. In 2005, amendments to the Nova Scotia *Municipal Elections Act* allowed for alternative voting methods to be introduced at the local government level, provided that the local government passed an authorizing by-law. In 2007, HRM council approved Internet and telephone voting[71] for the 2008 HRM municipal and school board elections as an additional voting channel during the advance voting period. The council established a number of goals for the Internet voting system, including increasing convenience (particularly for Halifax's older voters), potentially increasing voter turnout, improving cost effectiveness, and reducing the time required for vote counting and reporting.

Based on the success of the 2008 election, it was trialled again in a 2009 council by-election, and from the combined experience council approved its use again for 2012. In both cases it was also limited to the advance voting period.

Following an RFP ahead of the 2008 election, HRM entered into a four-year contract with a vendor to conduct all Internet voting. Prior to the 2012 election HRM conducted another RFP process. Three proponents met the requirements and HRM entered into a contract with a different vendor to conduct that election.

Process

All registered HRM voters are sent credentials (PIN) by mail ahead of the election. The provided PIN plus the voter's date of birth (DOB) were used for authentication credentials in 2008 and 2009. In 2012, officials added a password as a third credential to be used along with the PIN and DOB. In all three elections, voters were also required to complete a CAPTCHA challenge as part of the log in process.[72]

70 For more information about HRM's experience with Internet voting, see references #38, 48, 76, 146, 236, 278, 279, 289, 290, 291, 294
71 All subsequent references will be to the Internet voting component only.
72 The effectiveness of the CAPTCHA technology to prevent automated logins is debated by researchers.

In 2008, Internet voting was offered twenty-four hours a day during the three day advance voting period, in addition to traditional voting opportunities. In the 2009 by-election, it was expanded to five days and in-person voting was reduced to one location only. In 2012, Internet voting was expanded to 13 days prior to general voting day and in-person voting during the advance voting period was eliminated entirely. On general voting day only in-person voting was available.

The Internet voting system in Halifax enables voters to spoil a ballot using a "decline to vote" button on the same screen as the candidate choices. Voters may choose to vote online at different times and via different devices (e.g., phone, work computer, home computer) for each race they are eligible to vote in (e.g., mayor, councillor, school board trustee), as opposed to having to complete all ballots in a single session. A voter is only entitled to vote once in each race and voters cannot vote online for some races and in-person for others.

Halifax also established voter registration sites in libraries during the advance voting period to enable previously unregistered voters the opportunity to register and become eligible to vote (including online).

Results

It is suspected that not requiring voters to pre-register to vote online (only to already be a registered voter) was one of the reasons for the higher level of Internet voting turnout in HRM than in Markham and other jurisdictions that required secondary registration.

The significant increases in Internet voting turnout in 2009 and 2012 are likely due in part to the reduced number of in-person voting opportunities in those same elections (only one voting place in 2009, and no advance voting places in 2012). Ninety percent of all electronic votes were cast online and only 10% were cast by telephone.

While turnout overall is not increasing, 60% of all ballots cast in 2012 were cast online. This suggests that Internet voting is widely accepted by voters in Halifax and may be considered to be more convenient for a majority of voters than in-person voting opportunities.

	2008	2009 (district by-election)	2012
Population	~385,500	~385,500	~390,000
Eligible voters	279,326	12,476	298,209
Overall turnout (#)	101,116	4,391	110,114
Overall turnout (%)	36.2%	35.2%	36.9%
Internet voting registration (#)	N/A	N/A	N/A
Internet voting turnout (#)	~25,000	3,258	66,272*
Internet voting as % of eligible voters	9.0%	26.1%	22.2%
Internet voting as % of votes cast	24.7%	74.2%	60.2%
When offered	Three days during advance voting period; 24h/d	Five days from beginning of advance voting period to end of general voting day; 24h/d	13 days during advance voting period; 24h/d
Vendor	Intelivote		Scytl

*These figures include Internet and telephone voting. Internet voting accounts for 90% of all electronic votes cast, or approximately 59,645 ballots.

Truro, Nova Scotia[73]

Origins

In December 2011 the Chief Administrative Officer (and election administrator) and a representative of an Internet voting vendor made a presentation to council recommending the use of Internet voting in the October 20, 2012, local government election. Council took it under advisement and in April 2012 approved a bylaw permitting Internet voting and establishing that there would be no voting with paper ballots.

The goals of Truro were to increase voter turnout, improve convenience and access, and to try to reach younger voters while promoting the progressiveness of the town.

Process

All voting took place online and was offered over a nine-day period. All registered voters were sent a PIN by mail ahead of the election. This PIN plus the voter's date of birth were used for authentication credentials. Truro used the list of voters for the town provided by Elections Nova Scotia.

73 For more information about Truro's experience with Internet voting, see references #214, 233, 295, 296

In an effort to replicate the traditional social experience, and to assist older voters in the community, the city set up computers for voting in four prominent locations. The city also appointed nursing home staff as election officials to assist elderly voters resident in long term care facilities.

Officials maintained a Facebook election page where they provided the public with regular updates of the number of votes cast. The page also contained encouragements to vote and links to YouTube videos demonstrating how to vote online.

Results

Turnout in the 2012 election increased from 19% of eligible voters to 47%. While this is a significant increase, it may not be attributed solely to the introduction of Internet voting. For the same election, Truro officials conducted a new comprehensive education and outreach program. The local returning officer wrote an election-administration column in the local newspaper for the six months preceding the election. Topics varied, but at least one column was written about the introduction of Internet voting. It is believed that this outreach contributed to the positive reception of Internet voting by the media and by voters.

	2012
Population	~12,000
Eligible voters	9,680
Overall turnout (#)	4,549
Overall turnout (%)	47%
Internet voting registration (#)	N/A
Internet voting turnout (#)	4,549
Internet voting as % of eligible voters	47%
Internet voting as % of votes cast	100%
When offered	9 days during Internet voting; 24h/d
Vendor	Intelivote

Canada - Investigated and rejected

Kitchener, Ontario[74]

Circumstances for its consideration and why it was ultimately rejected

In June 2011, City of Kitchener council directed staff to investigate implementing an Internet voting option for the 2014 municipal election and report back on the issue by the end of 2012. On November 2, 2012, the City Clerk submitted a report to council recommending that Kitchener not implement Internet voting and on December 10, 2012, a committee of council agreed with the Clerk's report not to implement Internet voting.

74 For more information about Kitchener's consideration of Internet voting, see bibliography references #224, 238

The Clerk's report was fulsome and reflected consideration of many of the most significant benefits and challenges to implementing Internet voting.

The Clerk's report claimed that the overall cost of the system, including the cost of ensuring the system would be secure enough for candidates and the public to have confidence in it, would be too great, particularly when added to the cost of the existing paper ballot process. Further, the Clerk wrote that research suggests it does not increase voter turnout (particularly among younger voters), that it cannot be adequately scrutinized, that there is not an established Canadian standard for evaluating Internet voting systems, and that its legitimacy hadn't been tested in the courts.

Edmonton, Alberta[75]

Circumstances for its consideration and why it was ultimately rejected

In 2010, Edmonton city council first asked municipal staff to look into the possibility of implementing Internet voting for city elections. In February 2012 the capital region communities of City of Edmonton, City of St. Albert and Strathcona County submitted a joint proposal to the provincial Ministry of Municipal Affairs requesting permission to conduct a pilot project for the 2013 Alberta municipal elections. These municipalities wrote that their proximity, experience with advanced voting techniques, and size (one large, one mid-sized, and one rural/urban municipality) warranted a joint project. The original objective of a pilot focused on convenience.

Funded by the Ministry of Municipal Affairs, the City of Edmonton conducted a mock election using Internet voting technology from Scytl to evaluate voters' readiness to use Internet voting and to test the technology to see if it met the city's requirements. To avoid political opinions influencing the pilot, the city asked voters to vote on their favourite colour of jellybean.

There were no eligibility requirements for who could participate, but all voters were required to register with the city by completing an online registration form and uploading a copy of their ID. While the city stated it had hoped for a large number of voters, fewer than 500 individuals participated in the pilot.

Edmonton contracted with a third party to test the security of the Internet voting system used. When another group of computer security experts[76] requested permission to attempt to compromise the system, they were denied permission. The city reported that thirteen attempts to compromise the voting system were made, but that all were repelled. Of the thirteen attempts, five were invited and eight were not.

Satisfied with the Jellybean Internet Voting pilot, the City Clerk developed a review process with the Centre for Public Involvement (a City of Edmonton and University

75 For more information about Edmonton's consideration of Internet voting, see bibliography references #205, 218, 226, 248, 249, 250, 251, 252, 255, 297

76 These experts included: Jeremy Epstein, Barbara Simons, Ronald L. Rivest, and David Jefferson.

of Alberta group created for public engagement projects) to further assess the receptiveness of the city for Internet voting. This review included a survey of residents, roundtable meetings with stakeholders and, most prominently, a citizens' jury process.

The Citizens' Jury was made up of 17 (originally 18) residents of Edmonton selected at random from the previous survey respondents. In November 2012, jurists participated in one weekend learning session where they heard about some Internet voting benefits and challenges from practitioners, academics and vendors. Presenters to the jury put lots of emphasis on the social benefits to the city (to be seen as a leader in the field, civic pride, keeping up with other cities) if it adopted Internet voting. Jurists were not expected to become experts on Internet voting, but based on what they learned during the weekend were to give their opinion as to whether Edmonton should adopt Internet voting as an option for future municipal elections. The City Clerk indicated during the weekend that she would only recommend to Council that the city implement Internet voting in 2013 if the Citizens' Jury also recommended so. At the end of the weekend the jury, by consensus, enthusiastically recommended the city implement Internet voting at the 2013 municipal election.

In January 2013 the Clerk reported to council she was recommending Internet voting be adopted as another option for voting in the 2013 Edmonton municipal election. However, at the February 6, 2013, council meeting, council decided not to proceed with Internet voting. Council stated that it was concerned at the cost and security of Internet voting and the Mayor stated that convenience was not enough of a reason to implement it.

Ahead of the council meeting, an individual reported to the media he had registered more than once and cast a ballot under each registration instance. Although the way in which the voter registered multiple times was unrelated to the Internet voting technology, based on the deliberations of the council, the panel suspects this announcement contributed to the security concerns of council.

In March 2013, the Minister of Municipal Affairs announced that the provincial government would not authorize Internet voting for any Alberta municipality for the 2013 elections, but would continue to monitor Internet voting for future use.

Canada (federal)[77]

Circumstances for its consideration and why it was ultimately rejected

Since 2004, Elections Canada has been surveying Canadians on the subject of Internet voting to learn of their interest and concerns. In addition to this polling and being a supporter of Internet voting research generally, in 2008 Elections Canada, in its five-year strategic plan, proposed trialing Internet voting in a by-election by 2013. By 2009 it had refined its plan to conduct such a trial after March 2013. Such a trial was dependent on Parliamentary approval and was to be limited in scope to voting terminals used in a controlled environment, such as by military voters using a military network. Limiting the scope in this way would allow Elections Canada to control many of the Internet voting security and authentication issues.

Despite the interest in the pilot, the Chief Electoral Officer did not believe that Internet voting would become a permanent channel for voting in federal elections for at least three general elections.

In April 2013, after budget cuts took effect at Elections Canada, the Chief Electoral Officer announced that Elections Canada had no immediate plans for a pilot before the 2015 general election. In addition to budget pressures, the issue of authentication and concerns over data security, it is likely that current initiatives focused on significant changes to the voting process at the federal level may have factored into the decision not to conduct the pilot as originally planned. The Chief Electoral Officer reported to Parliament that Elections Canada will continue to monitor the issue and consider an Internet voting pilot project again after the 2015 general election.

Ontario[78]

Circumstances for its consideration and why it was ultimately rejected

In the context of broader legislative changes to the provincial *Election Act* that placed an increased emphasis on the issue of accessibility, amendments to the *Election Act* in 2010 required Elections Ontario to review alternative voting technologies[79] and report back to the Legislative Assembly by June 2013. The new legislation also permitted Elections Ontario to use alternative technologies in a general election, provided it met three conditions: that it was first tested in a by-election; that the Chief Electoral Officer recommended it, having first been satisfied as to issues of security and integrity; and that the Legislative Assembly approve it after holding public hearings.

77 For more information about Elections Canada's consideration of Internet voting, see references #135, 241, 242, 253, 263, 292, 323

78 For more information about Ontario's consideration of Internet voting, see references #123, 132, 210, 211, 287, 292

79 Alternative voting technologies was defined by Elections Ontario as: "a means of both casting and counting votes electronically, involving the transmission of ballots and votes via telephones, private computer networks, or the Internet". Elections Ontario shortened this to "network voting" and established that it was meant to refer to Internet or telephone voting. For consistency, this report will describe Elections Ontario's work as related to Internet voting.

Elections Ontario initially announced it would use alternative voting technologies in a by-election pilot project in 2012 to inform its research. Elections Ontario developed a business case for Internet voting that established very detailed requirements for an Internet voting system and used those requirements to put together an RFP for an "off-the-shelf" system to be tested in a by-election. However, in the spring of 2012, Elections Ontario determined that a pilot would not be feasible in 2012. Elections Ontario "determined that it would introduce more complexity and security issues, operational challenges and risk than originally anticipated" and that the organization did not have sufficient time "to determine whether these risks could be adequately resolved."[80]

In June 2013 Elections Ontario submitted its report on Internet voting to the legislature. The report stated that none of the current technologies met all of its implementation criteria (accessibility, individual verifiability, one vote per voter, voter authentication and authorization, only count votes from valid voters, voter privacy, results validation, and service availability) and so would not move forward with Internet voting at that time; however, it would continue to monitor the systems and processes that come forward against those criteria so that it could make a recommendation for Internet voting "when it is warranted".[81]

Other jurisdictions - Implemented

Estonia[82]

Origins

After the creation of a secure national electronic ID card in 2002, the Estonian government began investigating Internet voting in 2003 and in 2004 decided it would be piloted in the 2005 Local Government Elections. After deciding to go ahead with Internet voting it contracted with a private firm for the system's development. The initial goals of Internet voting were convenience and increasing voter turnout, particularly among youth.

The Estonian president challenged the constitutionality of the Internet voting system implemented due to a concern that the decision to allow an individual to cast more than one ballot contravened the principle of one person, one vote. However the Supreme Court upheld the Internet voting legislation, ruling that although a voter could cast more than one ballot, this process was only going to be used to protect the secrecy of the ballot, and ultimately only one vote per person would be counted.

80 Reference #292
81 Reference #292
82 For more information about Estonia's experience with Internet voting, see references #48, 136, 142, 152, 154, 166, 240, 254, 257, 276

Process

Estonia mandates a national ID card with a digital chip for interaction with government services. Card readers are widely available in public terminals and home computers. This card plus a unique PIN is used by voters to authenticate themselves for all government services, including voting.

Internet voting has been used for the 2005 Municipal Elections, 2007 National Parliamentary Elections, 2009 Municipal Elections, 2009 European Parliamentary Elections and 2011 National Parliamentary Elections.

Estonian elections are guided by three principles:

- secure digital authentication;
- "re-voting" (casting a ballot multiple times, but only the final ballot is counted); and
- supremacy of the paper ballot (a ballot cast in person on general voting day supersedes any electronic ballots cast)

Internet voting is only available for a limited number of days prior to general voting day and uses an electronic "double envelope" system comparable to the secrecy/certification envelope process used for absentee voting in B.C. provincial elections. The system does not use end-to-end verification methods and the voter cannot independently verify that their ballot was successfully cast.

Results

There were several key success factors to its implementation: a high level of computer literacy; high-level of computer access; the existing electronic ID card; political will; and a legal framework for Internet transactions. Access to the Internet is a social right of Estonians enshrined in legislation.

Use of Internet voting has increased significantly since it was first introduced, but after five elections it is still only used by less than 16% of eligible voters.

	2005 (municipal)	**2007** (national)	**2009** (local government)	**2009** (European Parliament)	**2011** (national)
Population	~1,346,000	~1,342,000	~1,340,000	~1,340,000	~1,340,000
Eligible voters	1,059,292	897,243	1,094,317	909,628	913,346
Overall turnout (#)	502,504	555,463	662,813	399,181	580,264
Overall turnout (%)	47.4%	61.9%	60.6%	43.9%	63.5%
Internet voting registration (#)	N/A				
Internet voting turnout (#)	9,317	30,275	104,415	58,669	140,846
Internet voting as % of eligible voters	0.9%	3.4%	9.5%	6.5%	15.4%
Internet voting as % of votes cast	1.9%	5.5%	15.8%	14.7%	24.3%
When offered	Three days; 24h/d	Three days; 24h/d	Seven days; 24h/d	Seven days; 24h/d	Seven days; 24h/d
Vendor	Cybernetica AS				

Norway[83]

Origins

In 2008, the Norwegian Parliament approved an Internet voting pilot at the request of the governing party. The pilot consisted of 10 municipalities offering an Internet voting option in addition to existing voting opportunities during the local government elections in September 2011 and was overseen by the federal Ministry for Local Government and Rural Development. The ten pilot municipalities were chosen by the Ministry to participate out of the 428 municipalities in Norway. Goals of the pilot project were to increase accessibility and convenience, improve efficiencies in election administration, and facilitate direct democracy. The Ministry contracted with Scytl to provide the Internet voting system for the pilot and with Norwegian technology company ErgoGroup (now EVRY) to provide an elections management system and integrate the two systems. The Ministry contracted with an independent auditor (Der Norske Veritas) to audit the software development process and with additional security auditors to review the source code.

Local government elections require a complex ballot due to the electoral system used in Norway (open list proportional representation)[84] and so potential efficiencies (time and resources) in counting and reporting were significant, as was the potential for a reduction in errors during counting. Each local government sets its own rules and procedures for counting (some count ballots by hand and others use vote tabulation machines). Each municipality involved in the pilot trialled the chosen technology in youth council elections and referenda six to twelve months ahead of the municipal elections.

83 For more information about Norway's experience with Internet voting, see references #38, 48, 82, 83, 84, 140, 141, 142, 148, 154, 173, 174, 184, 260, 273, 324, 329, 330, 331, 333

84 Open list proportional representation permits voters to express multiple preferences when marking the ballot.

Process

Ahead of the election, all voters in the pilot municipalities received unique verification codes by mail. Voters used their electronic national ID (MinID) to authenticate themselves prior to voting online. The online ballot was randomized and voters selected parties and candidates with a point-and-click interface. The system was designed to prevent over-votes, but did allow under-votes, including the casting of a blank ballot. Voters were shown their completed ballot before it was officially cast.

The voting system utilized E2E verification with return codes. Immediately after casting the ballot the voter received a verification code by SMS which could be compared against the unique verification codes mailed to the voter prior to the election. This enabled the voter to verify their votes were received as cast. Cryptography (digital signatures, hash functions and zero knowledge proofs) ensured each ballot was included in the counting and hashes of every ballot are published after the election to allow voters to verify that their vote was counted.

Voters were permitted to cast multiple ballots, but only the last ballot cast would ultimately be counted (maintaining the principle of one vote per person). Voters could also vote in-person at advance voting or on general voting day. Any ballot cast in-person superseded any ballots cast online. These two features meant that Internet ballots could not be counted until all in-person voters had been identified at the end of general voting day. Norwegian pilot municipalities used electronic strike-off systems in voting places to enable rapid identification of in-person voters and minimize delays prior to counting.

There were three phases of counting:

- **Cleansing:** removed duplicate ballots from a single voter and all ballots from an in-person voter, and removed personal identifiers associated with Internet ballot to enable the secret ballot
- **Mixing:** re-encryption of all cleansed ballots, which were then stored in a different order; this process severed any links with the state of the ballots during the cleansing phase and the order of ballots cast
- **Tallying:** decryption of the votes using keys distributed among multiple key holders (i.e. election administrators, stakeholders, etc.) and tallying the number of votes for each candidate

Results

Utilizing some of the more advanced options presented to them, over one thousand voters cast multiple ballots (the most any individual cast was five), and over 650 voters voted in-person after casting an Internet ballot. In all cases, the latter of the final ballot cast online or the in-person ballot was the only ballot considered for each voter.

Online turnout among youth (16-17 year olds) was found to be lower than other age categories.[85] Anecdotal evidence suggests that younger voters preferred to vote in-person for social reasons.

Contrary to expectations, researchers found no statistically significant reduction in the amount of time required to count ballots compared to control municipalities. Rather, experience from the previous municipal election was a stronger influence on the amount of time counting took. The number of counting staff in pilot municipalities was almost 70% lower than in control municipalities, however researchers could not attribute all this difference to the use of Internet voting.

At the national level, resources required to manage the Internet voting project in the ten municipalities were quite low – two staff for the entire pilot, with an estimate of three staff needed for all local government elections.

Norway considered the high level of use as an indication the Internet voting option was trusted by voters. Voter turnout and level of trust in Norwegian political institutions is already much higher than average. Researchers on behalf of the election administration conducted a survey of voters and stakeholders after the election. They found:

- Level of trust in counting was lower for Internet voting than traditional methods, but was still high ("85% indicated a great deal of trust or some trust" in Internet voting compared to 92% for hand-counting paper ballots and 94% electronically tabulated paper ballots)
- Receipt of verification code created confidence, even though the number of people who verified it was suspected to be low
- Most voters accepted the security as adequate, or didn't question it; researchers hypothesise that voters who were not satisfied simply used paper ballots
- Stakeholders from pilot municipalities expressed positive feedback, trust, and wanted it used again ("reserved optimism")
    - local officials expressed concern with the accuracy of hand-counting and machine-counting of ballots

85 Norway also piloted voting by 16-17 year olds in 20 municipalities during the 2011 local government elections. Four municipalities were involved in both the youth voting pilot and the Internet voting pilot.

- National stakeholders, including political parties and civil society organizations, were unanimously against future use of Internet voting:
    - felt it was not necessary (did not share local officials' concern regarding traditional counting methods);
    - felt that the average person could not understand or monitor the system; and
    - felt that confidence in electoral system could decrease if results are close

No official complaints related to Internet voting were filed during the pilot.

When no stakeholder stepped forward to conduct an independent audit into the Internet voting, the Ministry contracted with a third party to do so. The perceived conflict of interest regarding the audit being requested and paid for by the election administration was seen to be less of a risk than no audit at all.

The audit demonstrated that all votes received remained unaltered during the counting and reporting process, but it did identify a small number of technical issues. For example, nine ballots showed too many votes cast and so were not counted. This scenario should not have been technically possible. The vendor determined either that there had been a purposeful attempt by nine voters to forge an improper ballot, or an error had occurred whereby the same party or candidate was listed twice on the ballot. Due to the nature of the error it was impossible to distinguish after the fact which of the two scenarios occurred.

Parliamentary approval to conduct a second pilot of Internet voting during its September 2013 Parliamentary Elections was granted in April 2013. The same ten municipalities in the 2011 pilot were included in the 2013 pilot, as well as two additional municipalities, for a total of approximately 250,000 eligible voters. In leaving the decision to conduct the second pilot so late in the election cycle, the amount of time available to develop and test the updated system and document all of the new procedures was limited.

The 2013 pilot largely followed the same procedures used in the 2011 pilot. Improvements over the 2011 pilot included new voting software, a new encryption model, and the establishment of a results verification process. The Ministry also took additional steps to emphasize the transparency of the process. These steps included: publishing the source code and system documentation on the Ministry website; broadcasting a seminar for election observers on its website; and broadcasting the decryption and counting of Internet votes on election day.

A new Internet Election Committee was formed to supervise key aspects of the preparation and verification activities and had the authority to suspend or even cancel Internet voting in the case of irregularities in order to "enhance the transparency and accountability of the Internet voting".[86] However, observers found that the Committee members "were not conversant with the system and relied entirely on the Ministry's guidance and advice" and its ability to act as an independent oversight body was questionable.[87]

On the last day of Internet voting, the Ministry announced that a weaker level of encryption had been used for Internet ballots cast to date than was planned for. This meant that it was possible for system administrators with access to the electronic ballot box to decrypt the ballots without the need for the secret decryption key. To address this issue, the Ministry "tightened access restrictions to the servers holding the electronic ballot box by requiring a written authorization each time servers were accessed" and updated the voting client software with the proper level of encryption for votes cast after this error was identified.[88]

Like the 2011 pilot, the 2013 pilot also enabled voters to check that their ballot was cast as intended and recorded as cast by comparing a verification code sent to them by SMS after voting against the unique verification codes mailed to the voter prior to voting. In 2013, voters could also check that their vote would be included in the tally by comparing an encrypted version of the vote displayed to the voter after the ballot was cast with a record of all encrypted votes published to an Internet bulletin board. As voters were permitted to vote multiple times with only the last vote being counted, each vote would be recorded on the bulletin board. While the Ministry provided an opportunity for political parties and the media to verify the tally (universal verification), none chose to do so and the only body to do so was contracted by the Ministry.

In the 2013 pilot, 36% of registered voters in the pilot municipalities used Internet voting, up from 17% in the 2011 pilot.[89]

86 Reference #333
87 Reference #333
88 Reference #333
89 Reference #273

2011 Norwegian Pilot

	Bodo	Bremanger	Hammerfest	Mandal	Radoy	Re	Sandnes	Tynset	Vefsn	Alesund	TOTAL
Population											
Eligible voters	36,635	2,955	7,752	11,764	3,687	6,870	48,689	4,163	10,456	35,535	167,506
Overall turnout (#)	24,131	1,947	4,373	7,413	2,275	4,395	30,537	2,870	6,193	20,716	105,050
Overall turnout (%)	65.9%	65.9%	56.4%	63.0%	67.1%	64.0%	62.7%	68.9%	59.2%	60.0%	
Internet voting registration (#)	N/A										
Internet voting turnout (#)	7,014	408	1,132	1,466	771	987	8,246	907	1,334	5,473	27,738
Internet voting turnout as % of eligible voters	19.2%	13.8%	14.6%	12.5%	20.9%	14.4%	16.9%	21.8%	12.8%	15.9%	16.6% (avg)
Internet voting as % of votes cast	29.1%	21.0%	25.9%	19.8%	33.9%	22.5%	27.0%	31.6%	21.5%	26.4%	26.4%
When offered	31 days during advance voting; 24 hr/d										
Vendor	ErgoGroup & Scytl										

Geneva, Switzerland[90]

Origins

Swiss citizens are accustomed to voting remotely and often. Since vote by mail was first offered in the mid-1990s its use has increased to the point where 95% of all ballots cast in Geneva are now cast remotely. Swiss voters also have four to six opportunities a year to cast a ballot for various elections and referenda at the local, canton and federal levels, with the administration of all elections and referenda administered by the cantons. Switzerland also has a large number of overseas voters, for whom even vote by mail is not sufficiently convenient.

The cantons of Geneva, Neuchâtel and Zurich independently developed Internet voting systems with the financial assistance of the federal government.[91] Geneva began investigating Internet voting in 2001 and after a series of pilot referenda and non-governmental elections, a constitutional amendment was approved in a 2009 referendum[92] (using traditional voting methods) to allow for Internet voting in governmental elections.[93]

Internet voting is highly supported by the State Chancellor of Geneva. This is seen as contributing to the success of Internet voting's implementation and to the public's support of it.

The Internet voting system was intended to be "as easy, practical and safe as possible," reliable, include a voter verification capability and protect the secrecy of the vote.[94] The federal and state governments each set requirements for the Internet voting system and two ISO standards were also used as targets for information security management (ISO 27001 and ISO 27002). One of the federal requirements is that when Internet voting is available in federal elections it may not be used by more than 30% of eligible voters and must be approved by the federal government in advance.[95] In the canton of Geneva this means that Internet voting may only be available in selected municipalities or may only be available to overseas Swiss voters.[96]

When it authorized Internet voting, Geneva also established the Central Election Commission (CEC).

90 For more information about Geneva's experience with Internet voting, see references #38, 45, 48, 109, 142, 176, 191, 192, 195, 197, 261

91 While Geneva's system was developed and owned by the canton, Zurich contracted with Unisys and Neuchâtel contracted with Scytl for the development and operation of their systems.

92 February 8, 2009. 70.2% voted in favour of permitting Internet voting for Geneva.

93 Geneva conducted 11 votes using Internet voting during the pilot phase (2003-2008). After the 2009 referendum approving Internet voting for governmental elections, the pilot phase officially ended. Since this time, Geneva has conducted 20 more votes using Internet voting, though all but one have been for federal and cantonal referenda.

94 Reference #109

95 When Internet voting was introduced in Switzerland the cap was 10%, but over time it increased to 20% and in 2012 was increased again to 30%.

96 Internet voting has been used in 20 votes in Geneva, since 2009.

The CEC has oversight and inspection responsibilities related to Internet voting in Geneva. These responsibilities include the locking of the electronic ballot box and the generation of its encryption keys. The CEC also regulates the testing and auditing of Internet voting systems and controls access to the system and its source code by outside groups. It is required by law to conduct a full audit of its system every three years and to publish its results.

Geneva also hosts Internet voting for other cantons, including Bern, Lucerne and Basel-Stadt using its own Internet voting system. Under this model, the other jurisdiction provides its voters list to Geneva, which conducts the Internet voting and transmits the results back to the other jurisdiction for reporting.[97]

Geneva was not one of the four cantons chosen by the federal government to use Internet voting for overseas voters in the October 23, 2011, federal election. However, Geneva's Internet voting system was used in that election by voters in Basel-Stadt.[98]

Process

Under the Geneva system, all voters are mailed a card with authentication credentials. Voters use a PIN that is hidden under a "scratch-off" portion of the card (like a lottery ticket) along with their date of birth and city of origin (shared secrets) to log into the system. Geneva's system utilizes encryption and the double envelope method to prevent a link between the voter and the ballot, but does not use other security methods such as digital signatures.

To prevent voters from being able to sell their vote, voter verification methods only prove to voters that their vote was counted and does not include any indication on how it was marked.

Decryption of the voting results requires that representatives from the state chancellery, the CEC, the state election administration, the police and a notary are present. While the electronic ballot box is sealed, if the number of votes in the ballot box and the number of voters recorded as having voted do not match, an "integrity meter" will sound an alarm.

97 Zurich also offers its system to other cantons, but instead of administering the other canton's election itself, it provides a copy of its system to Unisys, the original developer, which administers the Internet voting for the canton.

98 The approved cantons were: Basel-Stadt, St. Gallen, Grisons, and Aargau.

Results

Geneva is one of the jurisdictions that believes Internet voting has had a positive effect on voter turnout. This is partially due to the high level of younger voters (18-39) who responded in a survey that they typically did not vote. Voters under 50 were also more likely to use Internet voting than any other channel, and 90% of voters who used Internet voting claimed they would likely use it again. Geneva has also reported a 20% increase in the number of registered overseas voters since Internet voting was introduced.

In its third report on Internet voting since 2006, the federal government stated that Internet voting would be expanded to the majority of overseas voters by 2015 and possibly to all Swiss voters at some point after its next report in 2017/18.

	May 15, 2011 (canton referenda)	November 4, 2012 (local government election)
Population	241,780	240, 484
Eligible voters	241,780	240, 484
Overall turnout (#)	~95,540	~67,336
Overall turnout (%)	39.5%	28%
Internet voting registration (#)	N/A	N/A
Internet voting turnout (#)	21,057	~10,100
Internet voting as % of eligible voters	8.7%	4.2%
Internet voting as % of votes cast	22.0%	15%
When offered	28 days during advance voting; 24h/d	28 days during advance voting; 24h/d
Vendor	State of Geneva	State of Geneva

New South Wales (NSW), Australia[99]

Origins

In March 2010, the New South Wales Parliament directed the New South Wales Electoral Commission (NSWEC) to investigate the feasibility of Internet voting for visually-impaired voters in the March 2011 State General Election. In July 2010, the NSWEC concluded that Internet voting would be technically feasible but difficult to implement for March 2011 State General Election. Legislation to provide Internet voting for this group of voters was introduced in November 2010, but was amended weeks later to expand the classes of eligible to include voters who would be unable to vote for reason of location (being more than 20km from a voting place or being out of the state on general voting day).

99 For more information about New South Wales' consideration of Internet voting, see references #99, 223, 306, 321, 332

The state's goals were to improve accessibility (allow independent voting by visually-impaired voters and improve convenience for remote voters), to reduce the likelihood of errors in marking the ballot (New South Wales uses a complex, preferential ballot and is legally obligated to provide Braille ballots for visually-impaired voters), and to reduce counting errors, cost and other issues associated with absentee voting.

Following a public tender process, NSWEC contracted with EveryoneCounts to provide the iVote Internet voting system used in the 2011 State General Election.

Process

In order to register to vote using the iVote system, voters were required to call NSWEC, verify their identity and confirm their eligibility for Internet voting. While on the phone the voter creates a PIN, which the system uses to create a voting credential (a hash based on PIN and other items) on the voting server. A unique, random voter number was also created by the system and sent to the voter via mail, SMS, SMS to Voice, or phone (phone option available for visually-impaired voters only). A letter was mailed to the voter's registration address on record with NSWEC to confirm that they did in fact register for Internet voting.

The voter number and PIN are required to cast a ballot. After the voter casts a ballot, the system creates a unique random receipt number and displays it for the voter on the device they used to vote. This number and their voting credentials can be used after the close of voting to confirm that their vote was received. However, because the voter cannot verify their vote during the voting period, there was no opportunity to vote again if a problem was identified. Further, as the voting receipt is issued during the voting transaction through the same channel as was used for voting, if the security of the voting process was compromised, the verification process would be similarly compromised.

NSWEC chose not to use E2E verification in the Internet voting system it implemented in 2011 "due to the emerging nature of the technology at that time". In its iVote strategy document prepared for the 2015 State General Election, NSWEC wrote that "full E2E where anyone can verify that all recorded votes are properly tallied…increases the complexity [and] reduces the ability of [voters], stakeholders and [NSWEC] to understand the system and be confident in its results".[100] In the proposed new iVote system to be used in NSW in 2015, the NSWEC will use a partial E2E approach. This approach will allow a voter to verify that their vote was received and NSWEC to verify "in aggregate" that all votes were counted as cast. NSWEC felt that the verification of results (both individual and overall) should be simple enough for voters to understand and voters should only have to rely on the expertise of NSWEC and appointed experts to trust that the proposed new iVote system works.[101]

100 Reference #321
101 Reference #332

Results

The legislation required an independent audit be conducted before and after each general election to ensure that the system was secure and the results reflected the votes cast. However, results for the first audit were to be provided to the NSWEC only "at least 7 days" before voting began and several weeks after iVote registration had begun. While this audit is separate from security reviews of source code, cryptography, infrastructure and processes and penetration testing that took place a month prior to the election, conducting an audit only seven days prior to the beginning of voting is not very much time to make changes if risks are identified. In fact, some risks that were identified by the security reviews and the pre-election audit remained outstanding during the election.

According to the auditor, late legislation meant "incomplete documentation, restricted test case formulation and compressed testing activities".[102] The auditor recommended an expanded level of testing for future events.

Five incidents occurred during the voting period, including one incident affecting 43 ballots that was not discovered until after the close of voting.

The NSWEC deemed the 2011 state election experience with Internet voting a success and the legislature has approved the use of Internet voting for the next state election in 2015. Procurement of an Internet voting system for that election began in July 2013. NSWEC intends to publish procedures, system architecture, voting protocol, security and source code reviews and post-election audits for the 2015 election to its website. It also has plans for increased stakeholder consultation, including a technical consultative group made up of outside experts that apply to participate. These technical groups will have access to the system's source code, but its use and members' ability to comment publicly will be limited so that "expert reviewers do not diminish the trust placed in [NSWEC] and the electoral process through sensationalised public comment". Beyond the technical consultative groups, public access to source code will be limited to those individuals and groups that can prove their expertise and are willing to sign a non-disclosure agreement.

The version of the system to be used in 2015 will improve the verification process. Voters will be able to access the content of their vote online or via an automated telephone system that reads back their vote. If their verified vote does not match the voter's intent, the voter can re-register and vote again. Re-registering automatically deletes their previous vote. The receipt numbers are to be published after counting to allow voters to verify their vote is included in the count, and all votes will be anonymized and published online to allow anyone to verify the tally of results.

102 Reference #99

	2011
Population	~7,210,000
Eligible voters	4,635,810
Overall turnout (#)	4,290,595
Overall turnout (%)	92.6%*
Internet voting registration (#)	51,103
Internet voting turnout (#)	46,864**
Internet voting as % of eligible voters	1.0%
Internet voting as % of votes cast	1.1%
When offered	12 days during advance voting; 24h/d
Vendor	EveryoneCounts

* Voting is compulsory in New South Wales

** 44,605 by Internet and 2,259 by phone

Other jurisdictions - Investigated and rejected

USA (military and overseas voters)[103]

Circumstances for its consideration and why it was ultimately rejected

Election administration in the United States for all three levels of government (local, state and federal) is conducted at the county level with guidance from the Secretary of State. As such, voting procedures can vary widely from county to county and from state to state. While Internet voting has not been implemented in a large-scale, binding governmental election to date, it has been the subject of significant amounts of research and a number of smaller pilot projects.

Internet voting in the United States has largely been focused on providing increased accessibility of the electoral process for U.S. military and overseas voters – two groups that have traditionally had difficulty exercising their right to vote due to the amount of time required to send and receive ballots outside of the country and unreliable postal services. The Federal Voting Assistance Program (FVAP), on behalf of the Secretary of Defense, administers the *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA), the legislation that governs the voting process for these two groups.

FVAP began investigating Internet voting in the late 1990s ahead of a pilot project in conjunction with the 2000 General Election. The 2000 pilot was conducted for eligible UOCAVA voters in South Carolina and four counties in Florida, Texas and Utah, up to a maximum of 50 voters per jurisdiction. Due to the various technical and administrative requirements for participation, including a requirement for the voter to be mailed a CD-ROM with the appropriate software and a request for voters to also mail a paper ballot as a backup, only 84 voters cast an Internet ballot.

103 For more information about the USA's consideration of Internet voting, see references #38, 48, 57, 94, 118, 120, 142, 264, 265, 266, 267, 268, 269, 270, 271, 272

Building upon the 2000 experience, the Secure Electronic Registration and Voting Experiment (SERVE) was intended by FVAP to be a larger scale Internet voting pilot for the 2004 General Election for UOCAVA voters in fifty-five counties from seven states. However, after spending $22 million on the pilot, the Department of Defense (DoD) cancelled the pilot ahead of the election due to a lack of public confidence in the system after security concerns were identified by computer scientists contracted to evaluate the system. The researchers concluded that there was "no good way to build [a secure, all-electronic remote voting system] without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough".[104]

The 2009 *Military and Overseas Voter Empowerment Act* (MOVE) required states to improve the voter registration and absentee voting process for UOCAVA voters, and authorized the DoD to conduct pilot projects to test technology that would assist UOCAVA voters. The MOVE Act also required the DoD to report to Congress on such tests with the assistance of the Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST).

Based in part on this legislation, West Virginia established its own Internet voting pilot for UOCAVA voters during the 2010 Primary and General Elections. The state qualified two Internet voting vendors which the eight pilot counties could choose between to provide the service for their voters.[105] After submitting an application, eligible voters were emailed a username and URL by either the election administrator or the vendor to access the system. Voters received a verification code that would enable them to confirm that their vote was included in the tally of votes cast, but did not identify the voter's choices. Of the 165 voters that applied, 125 voters voted online in the November General Election. While the counties did not report any technical issues with the voting systems used in West Virginia, based on concerns with Internet voting raised at a 2010 UOCAVA conference and the experience of Washington D.C.'s Internet voting test in September 2010, the Secretary of State recommended that further research into the issues related to Internet voting be conducted. West Virginia did not use Internet voting in the 2012 General Election.

Although its 2011 report on Internet voting security stated that "pilot projects should be encouraged,"[106] the most recent statement from NIST issued in May 2012 states that "additional research and development is needed to overcome [the challenges of auditability, malware and a lack of a public authentication infrastructure] before secure Internet voting will be feasible".[107]

104 Reference #264
105 Scytl was contracted by three counties and Everyone Counts was contracted by five counties
106 Reference #94
107 Reference #272

United Kingdom[108]

Circumstances for its consideration and why it was ultimately rejected

The UK has conducted three rounds of pilot projects involving Internet voting for local government elections – 2002, 2003, 2007. While the UK Electoral Commission does not administer the local government elections or the pilots, it is required by law to evaluate and report on them.

2002

In 2001, the UK Electoral Commission wanted to explore Internet voting, among other voting and counting innovations, in order to encourage voter participation and improve the efficiency and accuracy of how elections are administered. Five local governments agreed to participate in a pilot that offered multiple electronic voting opportunities that included Internet voting. Internet voting accounted for between 10 and 27 percent of all votes cast in these municipalities; however there was no substantive evidence that Internet voting led to improved turnout overall. Post-election research showed that Internet voting was more convenient to voters with disabilities. While voters and candidates expressed concern that Internet voting would be more susceptible to fraud, the Commission was not aware of any actual cases of fraud. The Commission's evaluation of this pilot was largely positive and its critiques were largely related to the management of the pilot scheme.

2003

In 2003, fourteen local governments piloted Internet voting as an additional channel for voting. Credentials were mailed by the local governments and were sent in either one mailing, or two (for added security), depending on the jurisdiction. Use of Internet voting ranged from 10 to 37 percent of all votes cast in these municipalities, with an average of 12.6%. The Electoral Commission's evaluation of this pilot was more technical and contained a number of recommendations related to security and reducing risk.

2007

In 2007, five local governments piloted Internet voting as an additional channel for voting. Voters were required to pre-register for Internet voting and the Electoral Commission believed that this likely contributed to a significantly lower use of Internet voting compared to the 2003 pilots. This time the Commission reported that while the pilots were broadly successful, there were concerns of accessibility, public understanding of the process and technical problems in one jurisdiction. The Commission also raised concerns about poor planning, rushed implementation and a lack of quality assurance and testing by the local governments that resulted in significant risk.

108 For more information about the UK's consideration of Internet voting, see references #38, 48, 60, 62

The Commission recommended that no further Internet voting pilots be conducted until a comprehensive strategy for Internet voting is developed and UK standards for evaluating Internet voting systems are set.

Netherlands[109]

Circumstances for its consideration and why it was ultimately rejected

Dutch citizens living outside of the Netherlands are entitled to vote by mail in Dutch elections provided they register their interest ahead of the election. Turnout among these voters abroad is typically low (~5% of 600,000 eligible voters). The Netherlands experimented with Internet voting in 2004 and 2006 as an alternative to vote by mail for these voters in order to improve accessibility and convenience.

2004

In 2004, the Kiezen op Afstand (KOA) (Remote Voting) system developed by LogicaCMG for the Dutch government[110] was trialed and used by 4,871 voters for elections to the European Parliament. Registered voters received by mail a unique login code and a list of candidates with a code for each candidate on the list. There were 1,000 variations of the list of candidates and codes. The voter would enter their login code and the candidate code when voting online to indicate their preference instead of seeing a visual representation of the ballot. Together, this meant that if the security of the voting system was compromised, an attacker would still not know how the voter intended to vote.

2006

In 2006, the government decided to test a different system for voters abroad. This system was created by the Rijnland District Water Control Board and known as RIES (Rijnland Internet Election System). RIES had been successfully trialed in a large scale pilot project and included vote verification elements. RIES also used cryptography and a traditional visual representation of the ballot instead of candidate codes.

109 For more information about the Netherlands' consideration of Internet voting, see references #102, 156, 304, 305, 325

110 The majority of the KOA source code was subsequently released by the Dutch government for use as an open source Internet voting platform.

Interested voters abroad were required to register to vote using Internet voting at least four weeks before the election. Voters were then mailed an instruction booklet and sealed authorization code with which to authenticate themselves. Dutch law permitted voters to request a replacement authorization code if the original was lost, but this process required the election administration to maintain a link between the codes issued and individual voters so that the original code could be deactivated, thereby compromising the secrecy of the ballot.

Further, it required more codes be created than eligible voters, meaning the election administration had to be trusted to protect extra codes and to only issue the extra codes in authorized circumstances.

Voters were given a receipt that they could use after voting closed to verify their vote was counted, though the receipt did not show how the voter voted. After voting ended, a codebook was published linking all potential receipt codes to candidate names, along with a list of all the receipts issued to voters. This process enabled anyone to tally the votes independently. However if a third party gained access to both the receipt and the voter's authorization code used to vote, they would be able to determine who the voter voted for. Similarly, if the codebook was not kept secure throughout the election, it also could have been used with receipts to compromise the secrecy of the ballot.

Although a much larger number of voters abroad (19,815) voted online in 2006, developers and critics of Internet voting agreed that RIES would not be a suitable system if Internet voting were ever expanded to all Dutch voters.

Public support of Internet voting dropped significantly after the 2006 election due to significant issues found with the reliability and security of the Direct Recording Electronic (DRE) voting machines used in Dutch voting places for in-person voting. These problems with DRE technology resulted in a very low level of trust in all voting technology. Also at the time of the 2006 election, it became evident that the Dutch government had become too dependent on the private sector companies that it relied on for the provision and support of the DRE voting machines. This dependency meant that the election administration could not exercise its responsibility over all aspects of the electoral process. In 2008 the Dutch government mandated that only paper balloting be used for the foreseeable future.

APPENDIX G - GLOSSARY

The definitions used in this glossary are intended to be plain-language explanations of the terms used throughout this report. The panel recognizes that the definitions provided may not be as comprehensive as those used by experts in the relevent fields.

Absentee voting	Voting other than in-person at a voter's assigned voting place; includes vote by mail.
Accessibility	The ease with which voters can exercise their right to vote.
Adjudication	A process for determining whether a ballot has been marked in an acceptable manner and for whom the ballot has been marked.
Advance voting	Day or days for voting prior to general voting day; the period during which vote by mail is offered is not typically referred to as advance voting.
Algorithm	A sequence of actions to perform to accomplish some task or solve a technical problem; the term is often used in the context of computer programming.
Audit	An independent pre- and/or post-election evaluation of an organization, system or process which includes quantitative and qualitative analysis.
Auditability	The degree to which the integrity of the overall system for voting and, ultimately, the results of the election, can be confirmed.
Authentication	The process of identifying an individual as an eligible voter (may include confirming whether or not an individual has previously voted in the same election).
BC Services Card	A form of government-issued photo identification that serves as a combination drivers license and government services access card. The card has an embedded chip and other security features that could potentially provide a secure voter authentication mechanism for remote Internet voting in the future. The BC Services Card was launched in February 2013.
Ballot anonymity	The inability to link a ballot with the individual who cast it.
Candidate representatives	Individuals appointed by candidates to observe voting and counting on behalf of candidates at a voting place. Candidate representatives make sure that election rules are followed and that the counting is done fairly. Also known as scrutineers.
Chief Election Officer	The senior election administrator responsible for the administration of the local government electoral process in a jurisdiction in B.C.
Chief Electoral Officer	The senior election administrator responsible for the administration of the provincial electoral process in B.C.
Certification envelope	An envelope used in administering absentee voting. Identifiable information about the voter is written on the outside of the envelope. A secrecy envelope containing a ballot is sealed inside the certification envelope. The certification envelope is used to ensure that the voter votes, and the ballot is counted, in the correct jurisdiction. Used as part of the double-envelope process.
Cleansing	A electronic process that removes duplicate ballots from a single voter prior to counting; used by some Internet voting systems as one of three phases of counting.
Credentials	Physical or electronic document(s) that proves a voter's identity; used in B.C. local and provincial government elections and most other jurisdictions to authenticate a voter prior to issuing a ballot.
Cryptography	The practice and study of encryption and decryption, whereby, for example, a message is encoded so that it can only be decrypted by those with one or more keys known only to the intended recipient(s).

Denial of Service (DoS)	An attempt to overwhelm a server's capacity with traffic so that it is unable to perform its usual duties and respond to its intended users.
Device	Any means by which a voter may cast a ballot for Internet voting (e.g., computer, tablet, smartphone)
Digital divide	Refers to the gap between those with regular, effective access to digital technologies and those without.
Digital signature	Encryption of a message using the sender's secret key which authenticates the identity of the sender.
Distributed Denial of Service (DDoS)	A Denial of Service (DoS) attack conducted by a large number of computers, typically controlled remotely through malware.
District Electoral Officer	The senior election administrator, appointed by the Chief Electoral Officer, responsible for the administration of the election in a provincial electoral district.
Double-envelope process	A process for authenticating a voter remotely while maintaining ballot anonymity.
Election administration	The organization or body responsible for the administration of elections in a jurisdiction; e.g., Elections BC, individual local governments.
Election administrator	An official within an election administration, such as the Chief Election Officer, Chief Electoral Officer, or District Electoral Officer.
Elections BC	The usual name for the Office of the Chief Electoral Officer. Elections BC administers the electoral process in B.C. This includes provincial general elections, by-elections and provincial referenda. Elections BC does not administer local government elections or referenda in B.C.
Electronic voting	A broad term encompassing Internet voting and any other electronic means of marking a ballot, casting a ballot, or vote counting. Includes optical scan counting machines and direct-recording electronic voting machines (touch screen voting machines).
Eligible voter	In B.C., an individual who meets the qualifications for voting; in some jurisdictions, an individual who is registered to vote, or registered for Internet voting.
Encryption	Any procedure used in cryptography to convert plaintext into an encrypted message in order to prevent any but the intended recipient from reading that data.
(Encryption / decryption) Key	In cryptography, a value which must be fed into the algorithm used to encode / decode a message.
End-to-end verifiability (E2E)	Cryptographic protocols that enable anyone to confirm that all ballots cast were correctly tallied, and to prove to an individual voter that their vote is included in the final tally; also known as universal verifiability.
Final count	The final consideration of ballots cast in an election. The results of the final count are the official results, barring a judicial recount. For provincial government elections, the final count includes a confirmation of initial count results as well as the counting of absentee ballots.
General Voting Day	The final day for voting; ballot counting and announcement of preliminary results typically take place at the end of this day; also known as voting day or election day.

Initial count	The preliminary counting of some or all ballots cast in a jurisdiction with results subject to final count; typically conducted at the end of general voting day; does not typically include the count of absentee ballots.
In-person voting	The traditional channel in B.C. whereby voters attend a voting place, get authenticated face-to-face by an election official, and cast a ballot on paper.
Internet voting	A voting method where votes are transferred via the Internet to a central counting server; also known as voting online.
Internet voting solution	Products or services provided to conduct Internet voting.
Internet voting system	Technology and processes used to conduct Internet voting.
Jurisdiction	A geographic location for which elections are conducted; e.g., Nanaimo, British Columbia, or Estonia.
Machine code	Code used by a computer to cause an operation. Machine code is converted from source code using an automatic translation program called a compiler.
Mail ballot voting	see *Vote by mail*.
Malware	Malicious software; software designed to interfere with a computer's normal functioning (e.g., viruses, trojan horses, spyware) (Merriam-Webster).
Mixing	An electronic process implemented prior to counting involving encryption and decryption which removes any links between a marked ballot and the identity of the voter who cast it; used by some Internet voting systems as one of three phases of counting.
Observe	The act of witnessing and assessing, but not intervening in, the proceedings of an election.
On-site Internet voting	A form of Internet voting that is conducted at controlled settings, such as voting places or kiosks established in high-traffic areas. Election officials may be available on-site to authenticate voters and ensure secrecy of the ballot.
Over-vote	Marking the ballot for more than the maximum allowable number of candidates; this results in the ballot being rejected for that race and no vote being recorded.
Paper balloting	Voting using tangible ballots made of paper; as opposed to electronic voting or Internet voting.
Personal Identification Number (PIN)	A number (usually secret) assigned to an individual and used to confirm identity.
Phishing	The practice of attempting to acquire authentication credentials or other personal information by posing as a trustworthy or legitimate entity.
Process validation	The requirement that the procedures, technology and documentation to be used for Internet voting be available to the expert panel for testing and review for an appropriate length of time before, during and after the system is to be used, and for policies and procedures to be in place to respond to issues that arise.
Protocol	A set of formal rules describing how to transmit data, especially across a network.
Receipt	A randomly generated code that can be used by the voter after casting a ballot to ensure the vote is received and processed correctly by the voting system.

Rejected ballot	A ballot that is rejected during the counting because it is unmarked, is marked in a way that does not clearly indicate the intention of the voter, or is marked in such a way that the voter could be identified.
Remote Internet voting	A form of Internet voting that allows voters to transmit their voted ballot from any Internet-connected device and location to which they have access, e.g., home/office computer, smartphone, tablet. For the purpose of this report, see *Internet voting*.
Scrutineer	see *Candidate representative*.
Secrecy envelope	In absentee voting, the envelope in which the ballot is placed prior to being sealed inside a certification envelope. The secrecy envelope ensures that the ballot cannot be linked to the voter whose information is on the certification envelope. Used as part of the double-envelope process.
Shared secret	A fact or idea that both the voter and the election administrator know, but that few or no other individuals will know.
Source code	The form in which a computer program is written by the programmer. Source code is written in a programming language before being converted into machine code for a computer to read and use.
Stakeholders	Individuals or groups with an interest or concern in the conduct of elections; e.g., election administration, voters, political parties, candidates, MLAs, council members, technology vendors.
Supremacy of paper	The principle in some jurisdictions that have implemented Internet voting, that a paper ballot cast in-person will supersede any ballot cast by the same individual by Internet voting.
Tallying	Counting the number of ballots for each candidate; takes place after they have been adjudicated.
Traditional voting	Voting channels currently used for B.C. local or provincial government elections; e.g., in-person, absentee, vote by mail.
Transparency	The ability of individuals, groups, or the general public to scrutinize the activities of election officials, voters, and other participants in the electoral process. Transparency is achieved when observers can see that the requirements of applicable laws are being followed and the process is seen to be administered consistently and fairly.
Under-vote	Marking the ballot for no candidate, or fewer than the maximum number allowed in the race; where only one vote was permitted, this results in the ballot being rejected; where multiple choices are permitted, the valid markings are still recorded; often this occurs on purpose to indicate a protest vote, but can also occur unintentionally.
Vendor	A company that provides Internet voting systems or services.
Vote by mail	A remote voting channel whereby voters receive their ballot and associated voting material by mail, mark the ballot independently, and return it to the election administration by mail (some jurisdictions permit the voter or a representative to pick up and/or return the ballot in person; also known as mail ballot voting in B.C. local government elections.
Voter verification/ Voter verifiability	Processes or protocols that enable a voter to confirm that their ballot was received, and in some cases, counted as cast; End-to-end verifiability (E2E) is an extension of Voter verification/Voter verifiability.

Voting channel	A method for voting; either in person, by mail, or Internet; also known as voting opportunity.
Voting opportunity	see *Voting channel.*
Voting place	A building or other location where in-person voting takes place.
Voting process	The series of steps involved in casting votes for an election. The voting process may vary between jurisdictions and between voting channels in the same jurisdiction.
Write-in ballot	A ballot used in voting for a candidate in an election where the voter writes the name of the candidate or the registered political party they wish to vote for in a large blank space on the ballot. Used in certain types of absentee voting in B.C.

Mailing address: PO Box 9275 Stn Prov Govt Victoria, BC V8W 9J6

Phone: 250-387-5305

Toll-free: 1-800-661-8683

Email: info@internetvotingpanel.ca

Website: internetvotingpanel.ca

Independent Panel on
Internet Voting
BRITISH COLUMBIA

Website: internetvotingpanel.ca
Email: info@internetvotingpanel.ca
Enquiries: 1-800-661-8683

8017 (14/02)