ELECTIONS BC

A non-partisan Office of the Legislature

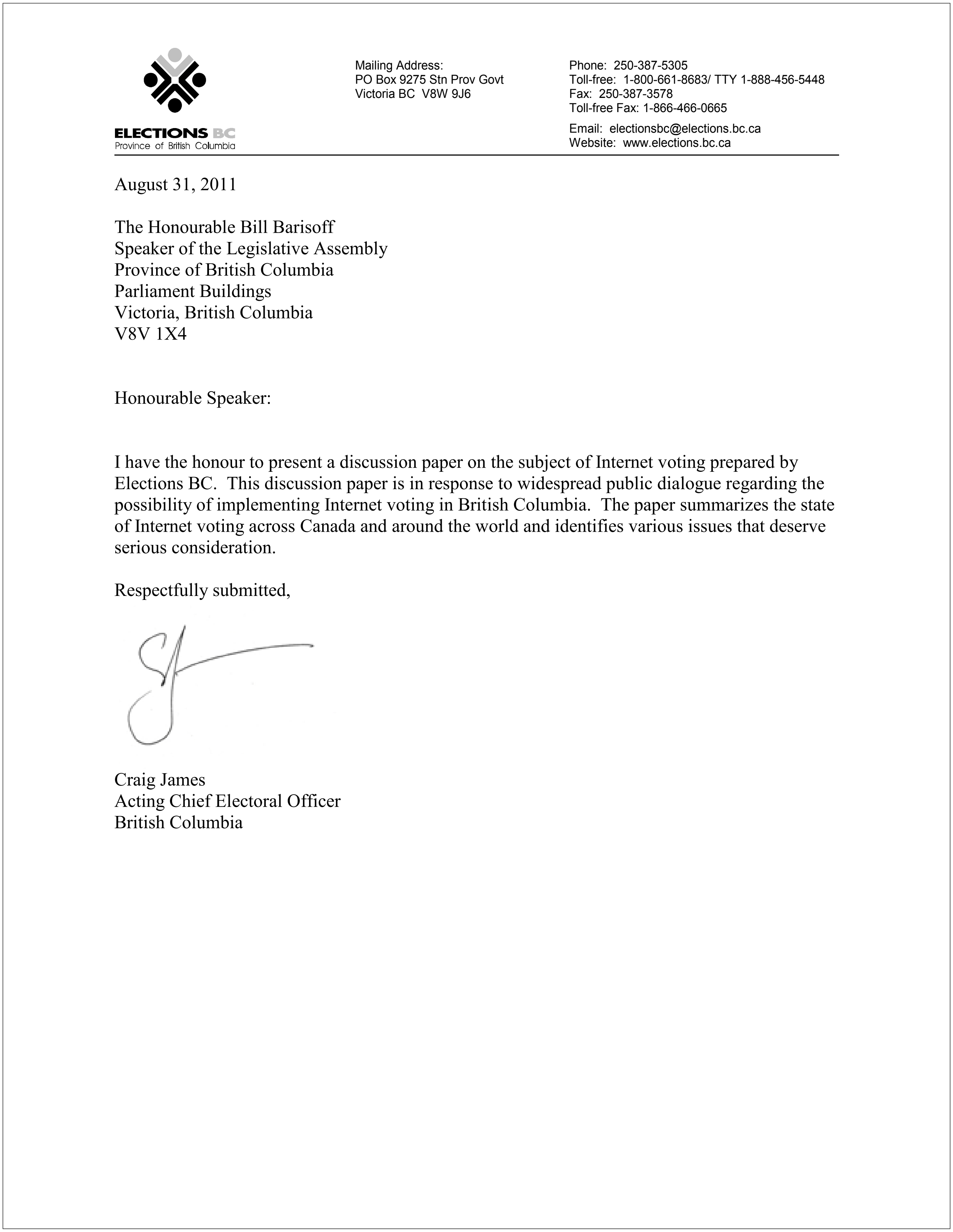
Discussion Paper: Internet Voting

August 2011

Discussion Paper: Internet Voting

August 2011

ELECTIONS BC
A non-partisan Office of the Legislature



ELECTIONS BC
Province of British Columbia

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 31, 2011

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Honourable Speaker:

I have the honour to present a discussion paper on the subject of Internet voting prepared by Elections BC. This discussion paper is in response to widespread public dialogue regarding the possibility of implementing Internet voting in British Columbia. The paper summarizes the state of Internet voting across Canada and around the world and identifies various issues that deserve serious consideration.

Respectfully submitted,

Craig James
Acting Chief Electoral Officer
British Columbia

Table of contents

1.0 Introduction

The Internet is changing citizen expectations around the speed and convenience with which all government services and elections should be delivered. We use the Internet to shop, bank, maintain our social and professional networks, and to find answers to our questions. Since 2004, when Elections BC introduced North America's first fully integrated online voter registration service, British Columbians have also been using the Internet to register to vote. It is natural that citizens are asking when they will be able to vote online, especially given that banking and other transactions requiring security to protect personal information are now routinely performed in the virtual world.

Policy makers are looking for ways to meet citizen expectations in terms of convenience and access to government services. While Internet voting is not currently an option in B.C.[1], the Premier has expressed an interest in further research on the topic. Other Canadian jurisdictions are also exploring various remote voting options to modernize and improve accessibility.

Ontario is planning to pilot Internet and telephone voting in a by-election in 2012. Pending Parliamentary approval, Elections Canada will trial Internet voting in a by-election in 2013. Internet voting is currently used by several municipalities in Canada.

Questions about Internet voting have sparked a vibrant debate, as policy makers, election administrators, computer experts, academics, private technology suppliers and interested members of the public discuss the potentially far-reaching implications of this form of voting for the security, transparency and integrity of voting and counting processes. Several prominent computer security and e-law experts have expressed concerns about the suitability of the Internet as a voting platform[2]. On the other hand, Internet voting has been used in elections of national-level governments in Estonia, and at smaller scales in several established democracies, including local governments in Canada.

This discussion paper addresses the question of what Internet voting may mean for B.C. through a review of the relevant literature. Our intent is not to propose a particular online voting solution for B.C., but rather to provide input to a future government committee or task force that may be created to delve further into the topic.

The potential benefits and risks of Internet voting are discussed in terms of seven of the core democratic principles that shape modern electoral systems: accessibility, equal voting power, secrecy, security, auditability, transparency, and simplicity.

[1] Electoral procedures in B.C. are defined by the province's Election Act, which would have to be amended to permit any form of electronic voting or counting.

[2] See, for example, Geist (2010), Jefferson (2011), Rubin (2002) and Schneier (2001).

Voting and counting processes in place in B.C. today reflect a delicate balancing of competing interests and values embodied in these principles.

Internet voting is about making the act of voting as convenient as possible and it holds great promise to improve accessibility, particularly to those who are absent from the jurisdiction, live in a remote area, or who have mobility issues.   However, this voting channel introduces risks to some of the fundamental principles of democratic systems. As policy makers consider a place for Internet voting, it is important that a balance is struck between competing principles, all of which are critical to electoral integrity, so that public confidence in election outcomes is maintained.

2.0 Internet voting defined

Internet voting refers to a voting method that transmits voted ballots[3] via the public Internet through a web browser or client application accessed through an Internet-connected personal computer, smartphone or tablet. There are two types of Internet voting.

On-site Internet voting is conducted at controlled settings, such as voting places or kiosks established in high-traffic areas (shopping malls, universities, etc.) where election officials may be available to authenticate voters to ensure the integrity of the device and software used and voters can vote in private.

The second form, remote Internet voting, allows voters to transmit their voted ballot from any Internet connection to which they have access (e.g. home/office computer, public library, hotel, smartphone).

While on-site Internet voting allows electoral administrators to exercise greater control over the voting infrastructure used on the client-side of the process, this paper focuses on remote Internet voting because it does not require voters to go somewhere to vote, and thus potentially reduces costs and maximizes the "convenience" factor that makes Internet voting particularly attractive.

[3] The term "voted ballots" refers to ballots that have been marked by voters with their selections.

3.0 Challenges with Internet voting

Elections BC is frequently asked why B.C. voters cannot vote online when online banking has been an option for years. The answer to this question highlights important elements of all democratic elections that make them distinct from commerce and provides a useful introduction to the issues discussed in this paper. Some jurisdictions have taken steps to address some of these issues in different ways; however all of these challenges need to be considered when contemplating an Internet voting system.

3.1 Security

Online banking was not introduced with the expectation that it would be a fraud-proof means of conducting banking transactions. The business case for online banking rests on the assumption that the degree of fraud is off-set by reduced operating costs and convenience benefits to clients. The reality is that online banking fraud is increasing at a rapid pace and banks expend substantial resources on insurance, reimbursing clients for fraud losses and on the on-going development of new strategies to address emerging security vulnerabilities[4].

3.2 Consequence

Elections are a cornerstone of democracy. The successful and accurate completion of each and every voting transaction is critical to public confidence in the integrity of elections, and ultimately, the legitimacy of those elected. Banking transactions, on the other hand, take place between private actors and the consequences of a dispute do not directly affect the rest of society.

3.3 Availability

If an Internet banking service is unavailable, clients can simply try again later. Elections are delivered according to a legislated calendar that allows for limited flexibility; for example, if General Voting Day is set as May 14, voting cannot normally be extended to May 15. In the case of an election, a service disruption for any number of reasons (e.g. denial of service attack[5] , hacking, software bug or hardware malfunction, power or network outage) could disenfranchise voters by delaying or invalidating their votes.

[4] The Canadian Council of Better Business Bureaus reports that identity theft is the fastest growing type of fraud in North America and estimates the cost at more than $2.5 billion per year to Canadian consumers, banks, credit card firms and other businesses (Canadian Council of Better Business Bureaus, 2010).

[5] A denial of service or DoS attack is an attempt to prevent legitimate users from accessing information or services by overloading the computers and network of the service provider with illegitimate requests for service.

3.4 Authentication and anonymity

Banking transactions are identifiable from end-to-end. They require user authentication through passwords and PINs and the client's identity follows the transaction through to its completion.

Voting is distinct in its requirement for both authentication and anonymity. A voting transaction must begin by authenticating the identity of the voter to confirm their eligibility. To preserve secrecy, the vote transaction must then be disassociated from the voter's identity. As well, voters do not receive a record that allows them to prove how they voted, as this would open the door to coercion and vote buying and selling.

3.5 Auditability

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

In a voting transaction, the requirement for secrecy means that a voter's identity is disassociated from the vote transaction after authentication. This makes it much harder to protect the system against fraud and to detect fraud that has occurred (Schneier, 2001).

If evidence of tampering with an Internet vote comes to light, there is no "before state" to return to in order to resolve the issue. By contrast, in the existing voting system, ambiguous results are resolved by having voter-marked and verified ballots reconsidered and counted again by another individual, such as a judge.

3.6 Transparency

Banks are private entities and it is expected that they will use proprietary and secret processes to protect online transactions.

Security through obscurity, however, is not acceptable in the context of an election where credibility is directly tied to transparency. When the voting public and observers can see that a system functions properly, they do not need to place their trust in election officials to the same extent. Transparency is achieved in the current system by having the acts of voting and counting take place in controlled physical locations, where observers and scrutineers representing the full political spectrum can see that procedures are followed. Technology encases voting and counting in a "black box", which has the effect of reducing transparency and, ultimately, public confidence.

3.7 Secrecy

Another concern with Internet voting that is not shared with banking is the requirement for a secret ballot. Because Internet voting takes place outside the controlled environment of a voting place, there is a risk that voters may be coerced or may engage in vote buying/selling schemes. This is possible because voters could allow others to observe how they mark their ballots. This risk has been accepted already in B.C. with remote postal voting, which has been used as the sole means of voting in two provincial referendums. However, in the context of a provincial general election, the *Election Act* limits postal voting to citizens in defined circumstances and only 0.2% of voters used this option in the 2009 General Election.

4.0 Experience with Internet voting

In spite of the challenges outlined in the previous section, many jurisdictions are using Internet voting in public elections. This section provides a high-level summary of experience with Internet voting in Canada, Europe, the United States, Australia and India. Several established democracies in Europe have made the necessary legislative and procedural changes to take voting online and have accumulated substantial experience over the last decade. Other countries, such as Canada, the U.S.A., Australia and India have proceeded more cautiously.

A summary of the key findings from a review of the literature related to the application of Internet voting in public elections is provided in the box below.

Summary of findings from implementations of Internet voting

- Tends to be implemented in jurisdictions with high rates of Internet usage and broadband access.
- Security and other risks have been controlled by trialling Internet voting as an additional channel layered on top of existing voting opportunities, limiting it to special groups of electors (e.g. overseas military), or focusing on lower levels of government and/or referendums.
- Never used as the sole voting channel in a public election.
- Used in Estonia in elections of national-level governments.
- Legislative framework is needed. In Estonia, the *Digital Signatures Act* supports online, digital authentication with citizen identity smart cards and passwords.
- Range of system designs and architectures are in use; reflecting local legislation, authentication strategies, and culture.
- No documented cases of hacking of Internet voting systems in a public election.
- Very popular with voters; surveys show that those who use Internet voting are very likely to use it again.
- Little evidence of a “digital divide” along socio-economic criteria; although use of Internet voting is correlated with computer knowledge.
- Popular with baby boomers and does not appear to be the answer to low youth participation.
- Impact on voter turnout is inconclusive. Its popularity tends to increase turnout in the part of the election in which it is used (e.g. advance voting), but overall turnout rates tend to remain unchanged.

4.1 Canada

4.1.1 Municipal

Canadian municipalities have been able to make a stronger case for the application of technology to electoral administration than have their provincial and federal counterparts. Local governments tend to have more complex ballots with larger numbers of candidates and multiple races, which can be time-consuming, challenging and expensive to count by hand. Since the 1990s, vote-counting technology has improved the speed and accuracy of the count and offered labour cost-savings for many local jurisdictions.

It is not surprising then, that Canadian municipalities have also been leaders in the introduction of Internet voting. Internet voting was first trialled by selected Ontario municipalities in 2003 and 44 Ontario municipalities now use the technology. Halifax and three Nova Scotia towns piloted a combination of Internet and telephone voting in their 2008 municipal and school board elections and Halifax used Internet voting again in a 2009 by-election (Alvarez, Hall, & Trechsel, 2009).

Municipalities in Ontario and Nova Scotia have seen an increase in participation in advance polls, where Internet voting was offered, but overall turnout has remained relatively constant[6]. The extent to which increased turnout at advance polls can be attributed to Internet voting is unclear, as advance voting has become increasingly popular at in-person voting opportunities over the last decade as well[7].

Canadian municipalities have selected a variety of commercial off-the-shelf Internet voting solutions from domestic and foreign suppliers. Markham uses a system supplied by a U.S. company, Election Systems and Software. Peterborough's system was developed by Toronto-based Dominion Voting Systems, and the systems in use in Nova Scotia were developed by Intelivote, a Nova Scotia-based company.

4.1.2 Federal and provincial

A formal dialogue among Canada's Chief Electoral Officers on the topic of e-voting began in 2009 with the establishment of the E-Voting Working Group. The group fulfilled its terms of reference in 2010 by developing a shared definition of e-voting and a set of guiding principles to be respected should the traditional model of elections be adapted to incorporate e-voting (uniqueness (one voter, one vote), privacy, transparency, and accessibility). Canadian jurisdictions are committed to sharing advice and experiences as jurisdictions move forward with plans to pilot Internet voting.

[6] For example, in Markham, turnout at advance polls rose by 300 percent when Internet voting was first introduced, but overall turnout was unchanged (Goodman, Pammett, & DeBardeleben, 2010).

[7] For example, advance voting accounted for 5.7 percent of valid votes in B.C.'s 1996 General Election, and 17.6 percent in the 2009 General Election.

At the federal level, an amendment to the *Canada Elections Act* in 2000 allows Elections Canada to trial electronic voting with the prior approval of Parliament. Aligned with its strategic objective to increase accessibility to the electoral process, Elections Canada has undertaken extensive research on the topic of Internet voting and, subject to the approval of Parliament, will offer an Internet voting option in a by-election in 2013.

In 2010, Ontario's *Election Act* was amended to permit the Chief Electoral Officer to trial an alternative voting method and to report to the Speaker of the Assembly on or before June 30, 2013 on the success of that trial. Elections Ontario plans to test an approach that combines remote and on-site telephone and Internet voting. The agency intends to have a fully-developed technical system in place by December of 2011, to pilot the solution in a by-election in 2012, and then to report to the Speaker in 2013.

The provincial government in Alberta amended its election laws in 2010 to make the voting process more open and responsive. Bill 7, the *Election Statutes Amendment Act*, introduced a range of electoral reforms, including provisions to trial new election procedures and equipment (which could include Internet voting) in a by-election with the approval of a legislative standing committee. Elections Alberta has not started to develop an Internet voting solution at the time of writing.

Premier Christy Clark, expressed support for Internet voting during the race for the leadership of the BC Liberal Party, arguing that it would help to engage more people in the political process and ultimately improve voter turnout (Ivens, 2011). However, Internet voting is not currently the official policy of the B.C. provincial government and it could not be used in a provincial election without amendments to the *Election Act*.

Interest in moving voting online is also building at the municipal level in B.C., with the province's two largest municipalities, Vancouver and Surrey, investigating the possible use of Internet voting in municipal elections in 2014, pending changes to governing legislation. The Province did not approve Vancouver's May 2011 request to pilot Internet voting in the November 2011 municipal elections due to the requirement for significant legislative change and risks to the integrity of the voting system, such as potential service disruptions, voter authentication issues and possible security threats.

4.2 Europe

European countries are the most advanced in the world in terms of their experience with Internet voting. Estonia, Switzerland, France, Germany, Spain, the Netherlands, and the United Kingdom have all trialled online voting. Norway is poised to deliver local government elections in some municipalities with an online voting option for the first time in September, 2011 and will offer nation-wide Internet voting by 2017 (Chowdhury, 2010).

4.2.1 Geneva, Switzerland

As early as 1982, the Swiss Parliament passed legislation to permit experimentation with alternative voting methods in the canton of Geneva. Later, in 2008, Parliament approved a constitutional amendment to permit Internet voting, which was ratified by citizens in 2009.

The conditions that paved the way for Internet voting in Geneva include:

- Emphasis on direct democracy that enables citizens to vote between four and six times per year
- Desire to improve turnout
- Experience with remote voting via an established postal voting system
- High level of Internet access
- Centralized, electronic voters list
- Large population living abroad
- Technologically progressive government

The canton of Geneva began Internet voting trials in 2001, and trials have subsequently been conducted in several other urbanized cantons in Switzerland. Trials in Geneva were initially limited to referendums and then expanded to elections (Goodman, Pammett, & DeBardeleben, 2010). Geneva has conducted the largest number of elections with Internet voting as an option for voters of any jurisdiction in the world (Alvarez, Hall, & Trechsel, 2009).

Internet voting is offered as an option for voters, along with in-person and postal voting. Voters access online voting via an e-Government service portal using a code printed on a voting card sent to them by post. Part of the code is kept secret under a scratch away layer, similar to those used on lottery tickets. Voters must also provide shared secrets (date of birth and municipality of origin) in order to authenticate themselves online to the election server.

[8] This “faithfulness effect” has been observed in Estonia (Alvarez, Hall, & Trechsel, 2009), as well as Geneva, Switzerland, and Markham, Ontario (Goodman, Pammett, & DeBardeleben, 2010).

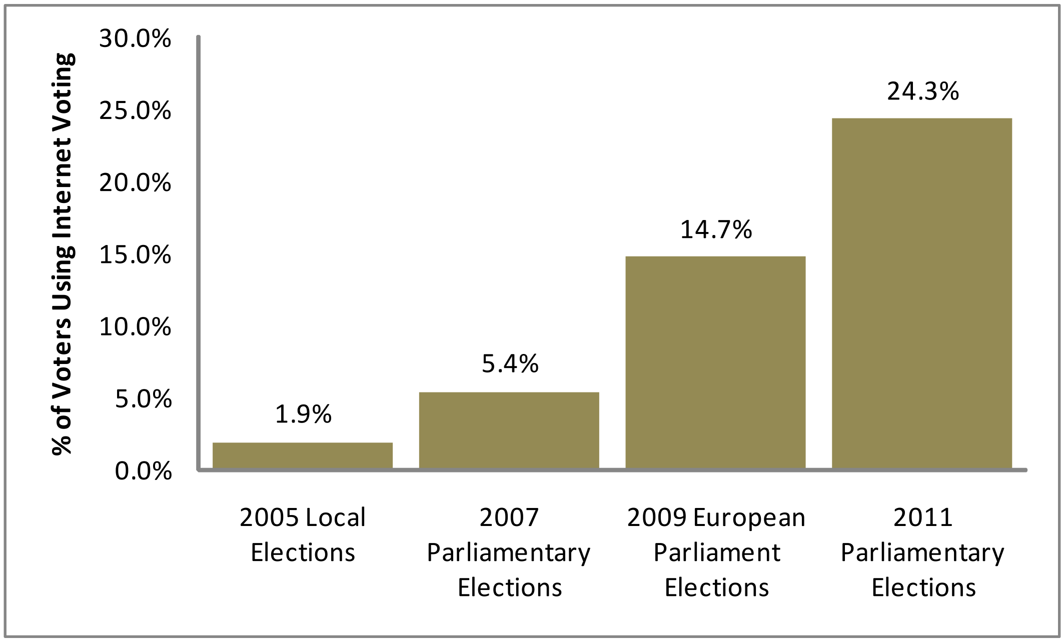
Internet voting has been well received in Geneva and has a strong and loyal following, particularly among voters under age 50. Post-election surveys suggest that Internet voting does not introduce political bias, nor bias by gender or education. However, there is evidence of a divide in terms of age and Internet competence.

4.2.2 Estonia

Estonia provides the only example of an application of Internet voting as an option for all voters at a national or supranational level of government, with parliamentary elections in 2007 and 2011 and European Parliament elections in 2009. In addition, Estonia offered Internet voting as an option in local government elections in 2005 and 2009. In the 2011 parliamentary elections, almost a quarter of votes cast were Internet votes.

In Estonia, the percentage of voters using online voting has risen steadily with each election since its introduction (see *Figure 1*).

Figure 1: Percentage of Voters Using Internet Voting in Estonia



Source: (European Parliament, 2011)

Researchers have also detected a strong “faithfulness” effect, meaning that those who vote online are highly likely to do so again in subsequent elections[8].
Some of the conditions that laid the groundwork for a successful implementation of Internet voting in Estonia include:

- Widespread Internet and broadband access
- Citizenry used to accessing government services via the Internet
- Identification system that permits digital authentication
- Supportive political culture
- Legal structure that addresses Internet voting (Alvarez, Hall, & Trechsel, 2009).

The approach in Estonia layers Internet voting as an optional “channel” on top of the traditional, paper-based voting process. Voters have three options to cast their ballots: 1) vote via the Internet during the Internet voting period (a subset of the advance voting period); 2) cast a paper ballot during the advance voting period; or 3) vote on election day with a paper ballot.

A key design feature of the Estonian model is that voters can cast multiple Internet votes and they can also vote with a paper ballot during the advance period or on election day. The last Internet vote cast is the one that is counted, unless the voter casts a paper ballot, in which case the electronic vote(s) is nullified and the paper ballot stands as the ballot of record. In order to implement this approach, a voter’s identity must remain associated to their voted ballot until a determination is made regarding whether the Internet vote should be counted. This system of multiple voting is an innovative yet administratively challenging means of protecting voters from coercion and vote-buying schemes to which they may be vulnerable in a remote voting setting.

4.2.3 Norway

Norway, an established democracy with 3.6 million registered voters, presents a valuable case-study for B.C. policy makers and election administrators interested in pursuing Internet voting. Norway plans to use Internet voting in some municipalities during its 12 September 2011 local elections (Nore, 2010). These elections will be the first step in a larger plan to implement Internet voting as an option for all voters in Norway’s 2017 parliamentary elections.

The Norwegian government recognizes the importance of building public trust in new voting systems (Nestas, 2010). Openness is one of its strategies for fostering public confidence in the ability of remote Internet voting to achieve a trusted result. All of the documents describing the architecture and technical matters related to the system, as well as the source code have been made available for public review (Chowdhury, 2010).

The system has a number of innovative features that allow voters to verify that their ballots are received as cast and that reduce reliance on the security of voters' personal computers. This is accomplished through the use of two independent channels: one to transmit the vote and another to confirm that the vote was received as cast. Voters cast their ballots using a remote computer and receive confirmation of how their vote was cast through SMS messaging on their mobile devices[9]. The idea is that if the voter's computer has been corrupted, the voter will be able to identify the issue and vote again (Ansper, Heiberg, Lipmaa, Overland, & van Laenen, 2011).

Internet voting will be offered during the advance voting period in Norway. If, prior to voting day, evidence comes to light that the system has been compromised, the fall back will be to paper voting on voting day.

4.2.4 European countries moving away from electronic voting

Some European countries, such as the Netherlands, the United Kingdom and Germany, have experimented with online and /or other forms of electronic voting and counting and have decided to discontinue or restrict their use in the future. These decisions reflect concerns with security, as well as the loss of transparency and auditability in voting and counting processes that could previously be readily observed by people with no special technical skills.

In the Netherlands, for example, Nedap/Groenendaal voting machines[10], which were used to capture approximately 90 percent of Dutch votes, were decertified on October 1, 2007 in response to a 2007 report of the Netherlands' Election Process Advisory Commission. The report argued that the principles of transparency, verifiability, and free and equal suffrage cannot be adequately safeguarded in the context of various forms of electronic voting, including Internet voting. Voting using paper ballots was identified as the preferred option on the grounds of transparency and verifiability.

In considering the future application of technology to voting and counting processes in the Netherlands, the Commission supported the use of ballot printers in the voting place, which allow voters to record their choice electronically, and to verify their choice on a printed ballot. The printed ballot could be stored for hand counting or scanned using optical character recognition technology and tabulated electronically. The Commission also argued that the application of Internet, postal and/or telephone voting should be limited to two classes of voters to support the principle of access in their cases: those unable to attend to vote at a voting place due to physical impairments and those voting from abroad (Election Process Advisory Commission, 2007).

[9] Confirmation via SMS is provided in the form of a candidate code as opposed to a plain text receipt. Voters are able to interpret the candidate code using information provided via the postal system at the start of the election. This ensures that voters cannot easily show others how they voted.

[10] This is a form of direct recording electronic (DRE) voting machine, which records, stores and tabulates votes electronically without producing a paper ballot for voter verification.

In the United Kingdom, the decision to discontinue use of electronic voting followed a series of trials of a range of electronic voting technology at the local government level. The UK Electoral Commission expressed concerns about transparency and security and noted that the majority of those who voted electronically were likely to have voted anyway via another channel, raising questions about value for money (The Electoral Commission, 2007).

Germany used electronic voting machines in voting places from 1999 to 2009, when the Federal Constitutional Court ruled the use of these machines unconstitutional. The Court found that the computer controlled voting machines used in the 2005 Bundestag election did not comply with the constitutional requirement of the principle of the public nature of elections, which prescribes that all essential steps of an election must be subject to the possibility of public scrutiny. This means that voters need to be able to verify, without detailed technical knowledge, that their votes are recorded and counted as cast. This is considered to be essential to ensuring the trust of the electorate in the correctness of the result (Federal Constitutional Court, 2009).

4.3 United States

Jurisdictions in the United States are proceeding cautiously with Internet voting. There have been four major trials of Internet voting, including presidential primaries in 2000 in Alaska and Arizona, the 2000 presidential and congressional elections through the Federal Voting Assistance Program's Voting Over the Internet program, and the 2004 Michigan Democratic primary.

Strong concerns have been raised by computer security experts in the United States about the potential for an Internet voting system to be targeted for a cyber-attack and the challenges in protecting such a system[11]. The Internet Policy Institute conducted a study of Internet voting in 2001 and concluded that "remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed," (Internet Policy Institute, 2001).

It is, therefore, unlikely that Internet voting will be endorsed by the federal government in the United States in the near future. Internet voting is however being implemented incrementally at the state level, largely to support overseas military and other American citizens living abroad. The United States has a relatively large overseas population and many states have experienced issues with the distribution of ballots in sufficient time to allow voters to return their voted ballots by legislated deadlines. In 2010, 33 states were using Internet voting to support military and overseas voting (Barnes, 2010).

[11] See, for example, the critique of the US Department of Defence's Federal Voting Assistance Program (Jefferson et al., 2004).

4.4 Australia

Online voting was trialled with overseas Australian Defence Force personnel in the 2007 federal election. The goal was to address the challenges faced by overseas military in returning voted ballots by post in time for counting. Overseas defence personnel were issued a unique PIN to access a voting application via a secure Intranet.

A report by the Joint Standing Committee on Electoral Matters recommended that the trials be discontinued in 2010 for a number of reasons (Joint Standing Committee on Electoral Matters, 2009). Although the uptake of online voting was reasonably high (1,511 personnel out of a possible 2,515, or 60%), the average cost per voter for the online option ($1,159) was considered expensive relative to the cost of other votes ($8.36) in the 2007 federal election.

The standing committee also considered the remote, online voting system to be less transparent than the postal voting option. In its recommendation to discontinue the use of online voting, the committee concluded that, on balance, the paper-based postal vote system is more reliable and imposes fewer burdens on defence force personnel than an online system with a paper back-up.

4.5 India

India uses electronic voting machines in voting places, but has not adopted online voting at the national level. India's Unique Identification Authority is laying the groundwork for online authentication for government services by issuing unique identification numbers to all Indian residents. The Authority began issuing identification numbers in 2010 and plans to issue 600 million numbers through its network of registrar offices located throughout the country by 2015 (Unique Identification Authority of India, 2011).

Interest in online voting is growing at the state-level in India, and the State of Gujarat is the first to trial Internet voting. The first trial was carried out in September 2010 and the system was used again in municipal elections held in April 2011. The solution used by the State of Gujarat is developed by Scytl, a well-established Internet voting solution provider based in Spain (Verified Voting, 2011). In the April 2011 election, 77.16 percent of registered voters cast their votes online, either from their home computers, or from kiosks (Alootechie, 2011).

As jurisdictions across Canada begin to offer Internet voting, and as Canadians become increasingly comfortable transacting business online, the provincial government in B.C. is likely to come under increased pressure to make similar options available in provincial elections and referendums. This section considers different rationales for adopting Internet voting.

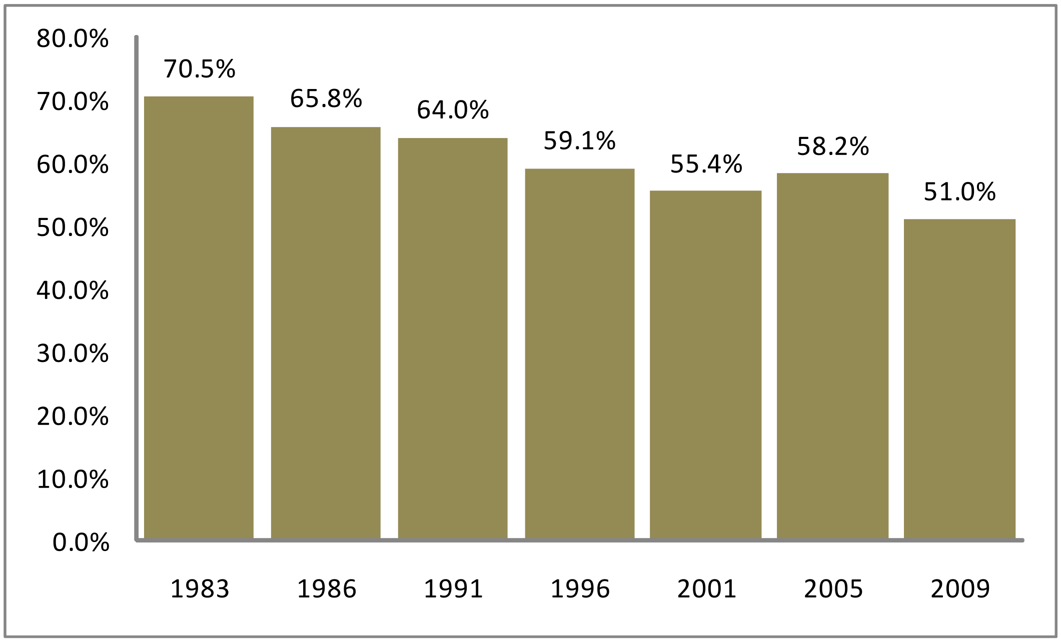
5.0 Rationales for Internet voting

5.1 Higher turnout

Voter participation in modern electoral democracies has reached record lows across the industrialized world and justified or not, this trend is a strong driver of interest in Internet voting. In the 2009 provincial general election in B.C., just over half of eligible voters voted (55.1 percent of registered). The proportion voting at the federal level in 2011 was slightly higher, at 61.4 percent of registered voters (Elections Canada, 2011).

Figure 2 shows the proportion of eligible voters participating in B.C. provincial elections declining from 70.5 percent in 1983 to 51.0 percent in 2009. The 2009 general election was the first since 1986 where the absolute number of voters declined from the previous election, as 122,808 fewer voters voted. Turnout is particularly low among younger voters, with only 26.9 percent of eligible voters aged 18 to 24 voting in B.C.'s last provincial general election (Elections BC, 2010).

Figure 2 : Voter turnout as percentage of eligible voters in B.C. provincial general elections



Source (Elections BC, 2010)

There is inconclusive evidence regarding how Internet voting affects overall turnout. The question is whether votes cast over the Internet are substitutes for votes that would have occurred through other channels, or if it generates new votes. A host of factors influence turnout from one election to the next, making it challenging to isolate the effect of any one.

After introducing online voting, it is common for jurisdictions to experience a rise in participation during the particular period in which Internet voting is available (e.g. advance voting). Take the Town of Markham in Ontario, for example, which saw a 300 percent increase in advance voting turnout in 2003 after the introduction of online voting. In spite of this dramatic increase in advance turnout, overall turnout remained constant. A total of 10,639 voters cast their ballots online in the 2006 Markham election, representing 18 percent of all votes cast (Goodman, Pammett, & DeBardeleben, 2010).

It is not possible to solely attribute an increase in advance voting turnout to the addition of online voting during the advance voting period. Advance voting has become increasingly popular during the last ten years in many jurisdictions that have not introduced online voting. For example, in B.C.'s 2005 General Election, turnout at advance polls was 82 percent higher than in 2001, and it rose again by 45 percent between 2005 and 2009. This change is attributable to increased awareness of the convenience of voting during the advance period, and as was the case in Markham, increased turnout during the advance period was not a harbinger of increased overall turnout in B.C. provincial elections.

Estonia has seen positive movement in turnout since the introduction of Internet voting. Prior to the introduction of Internet voting, 58.24 percent of eligible voters participated in the 2003 parliamentary election. After the introduction of Internet voting in 2007, turnout increased to 61.9 percent, and again to 63.5 percent of eligible voters in the most recent parliamentary elections held in 2011 (Kripp, 2011).

Though the trend appears promising, using statistical techniques to isolate the effect of the first use of Internet voting in Estonian parliamentary elections, Bochsler (2010) concludes there is no causal relationship between the increase in turnout and the new voting channel. The study finds that the increase was attributable to other factors, such as the introduction of the Estonian Greens party and that, for the most part, online votes substituted for votes that would have been cast at polling stations in the absence of an Internet voting option. Similar conclusions were drawn by the UK Electoral Commission (2007) in their review of Internet voting pilots conducted at the local government level in England and Wales in the spring of 2007.

There is also mixed evidence regarding the ability of Internet voting to engage young voters in democracy. In fact, the Internet voting option appears to be particularly attractive to baby boomers. In Estonia, for example, young voters consistently account for 10 percent of Internet voters, whereas voters over 55 account for 18 percent (Kripp, 2011). In Peterborough, Ontario, 70 percent of online voters were 45 or older and the highest rates of usage were reported for those in the 55 to 64 age category (Goodman, Pammett, & DeBardeleben, 2010).

More technologically savvy voters should tend to use the Internet, and it follows, therefore, that a high proportion of youth who vote will select an online option over other voting channels. Whether the option to vote by Internet will entice new young voters to become more active participants in democracy remains a question. Some survey evidence from Estonia (Alvarez, Hall, & Trechsel, 2009) and Geneva (Goodman, Pammett, & DeBardeleben, 2010) shows that approximately 11% of voters who used the Internet to vote would otherwise have abstained, suggesting that the potential exists for the Internet to draw in some new voters.

5.2 Convenience

One rationale for Internet voting is found in the convenience it brings to the voting experience. Eighty-five percent of Estonian voters who cast their ballot online said they did so because it was convenient. Further, almost a quarter of online voting activity took place outside the voting hours offered by traditional opportunities (Alvarez, Hall, & Trechsel, 2009).

Policy makers can be confident that if they build an Internet voting system, voters will use it. A national poll conducted for Elections Canada in 2009 found that 64 percent of respondents from British Columbia reported they would either be “somewhat likely” or “very likely” to vote online in a federal election if such an option were available (EKOS, 2009). The experience from jurisdictions that have offered Internet voting is that growing numbers of electors choose it over traditional, in-person options with each subsequent election (see *Figure 1*, for example). There is also a strong tendency for voters to use Internet voting again after trying it once (Goodman, Pammett, & DeBardeleben, 2010 and Alvarez, Hall, & Trechsel, 2009).

Given the delivery and return time needed for voting via the postal service and the requirement for ballots to be received by the close of polls, an Internet option could enhance voting convenience for populations traditionally served by postal voting. These include: those who are unable to attend to vote at a voting place, such as overseas military or others who find themselves out-of-province during an election, people with disabilities, and people residing in remote communities or institutions. Survey results from Estonia suggest that Internet voting facilitated access to the polls for voters living in remote areas of that country and that the option saved these voters considerable time (Bochsler, 2010).

People with disabilities may prefer Internet voting over traditional, in-person voting or voting with the assistance of technology in the voting place. Advanced, adaptive computer technologies are available to assist with mobility, hearing, and visual impairments, as well as learning disabilities. People with disabilities may prefer to use their own customized set-up, incorporating the adaptive technologies necessary to allow them to use their home computer, as opposed to a more standard technology available at a voting place.

5.3 Cost savings/fewer errors

Depending on the scale of implementation and the nature of elections in a given jurisdiction, Internet voting also has the potential to offer cost-savings and to reduce errors in voting and counting. Cost savings may be achieved if Internet voting replaces traditional, in-person opportunities.

However, it is assumed that, should Internet voting be introduced to B.C., it would be added as an optional layer on top of the existing system, perhaps replacing or complementing one or more of the current absentee opportunities. In this context, overall election costs would increase.

If, at some point in the future, Internet voting were to replace in-person voting, there could be substantial labour cost savings. In 2009, approximately $11.5 million was paid in fees to the 37,000 election officials hired to deliver the provincial general election.

Arguments to automate voting and counting to reduce voter- and election official-error have limited applicability in the B.C. context. With the first past the post electoral system that is currently in place, voters mark their ballots with a single ✘ or ✔ for their preferred candidate. This makes it easy for voters to vote and for election officials to count, and means that error rates in these two areas are low[12], leaving little to be gained through automation.

Automated counting has value where voting is by preferential ballot, such as what was proposed with BC-STV. In this context, there are multiple selections on a single ballot and the electronic capture of votes would allow for an automated count and faster delivery of an accurate result.

[12] Only 0.7 percent of ballots considered in the 2009 General Election were rejected (11,025 /1,651,567). Reasons for rejection included: voter intent unclear, identifiable mark on the ballot, or ballot left blank.

6.0 Current voting process in B.C.

Before discussing considerations for Internet voting in the B.C. context, it is helpful to explain the current voting process. The voting process in B.C. is an example of established and well-tested procedures that uphold the basic principles of electoral integrity and transparency and have, accordingly, earned significant public trust. B.C. is widely considered to have one of the most accessible electoral processes at the provincial or federal level in Canada. Although it is a traditional, paper-based system, generous absentee provisions make it as close to a "vote anywhere" model as can be found in Canada. Voters are not constrained to vote at their assigned voting place; they can vote at any voting place during an election.

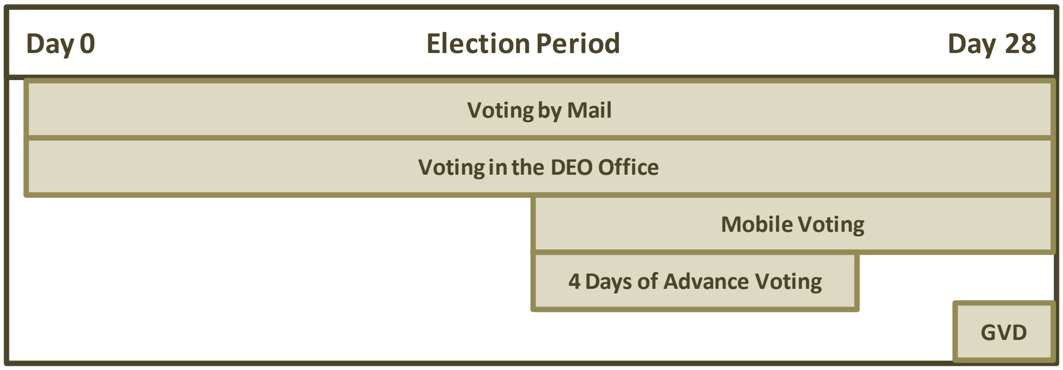
In a provincial election, B.C. voters have opportunities to cast a ballot from the day the writ is issued, to the close of polls on General Voting Day (GVD) (see *Figure 3*). Well before nominations close on Day 10 of the 28-day election period, voters can vote by mail or in any district electoral office throughout the province. In addition, voters can vote at any advance voting place over the course of the four days designated for advance voting or at any general voting place on GVD.

Other accessibility features of the system include:

- time off from work on GVD to vote
- on-site (mobile voting) in situations where voters cannot attend to vote at a voting place (e.g. long-term care facilities, hospitals, correctional facilities, and remote work camps).
- registration in conjunction with voting
- voting materials translated into a variety of languages
- lists of candidates and referendum questions in Braille, devices to allow voters with visual impairments to vote independently, and options at the voting place for translation and assistance with marking a ballot

One of the strengths of the current system is that it is transparent and easy for everyone to understand. The system is open in all respects, except of course for the protection of the secrecy of the vote. Voters are confident that the ballot they mark and personally deposit in the ballot box will be included in the count and interpreted accurately under the watchful eye of scrutineers representing all political views.

Figure 3: Availability of voting opportunities in B.C.'s current system



GVD (General Voting Day)

It would be extremely difficult, if not impossible, for malicious individuals to interfere with a ballot box election such as this on a large scale. Those with intent to commit fraud are limited in what they can do because voting takes place in a distributed network of controlled, physical environments in an atmosphere of almost complete transparency. Simple to execute and well-established standards of electoral administration also help to ensure against fraud. For example, ballot boxes are shown to be empty at the start of voting and are immediately sealed at the close of voting, scrutineers are welcome and encouraged to observe voting and counting processes, and election officials are required to work in pairs. If the race is close or there is any question regarding the accuracy of the count, voter-verified paper ballots can be reconsidered and counted by another person (e.g. a judge).

7.0 Changing the electoral process

Over the years, the B.C. government has adapted how elections are administered to reflect shifts in societal values and advances in technology. With the 2009 General Election, for instance, authentication standards were strengthened for in-person voting and accessibility was enhanced by increasing the hours available for advance voting. Election administration is a business of details and changes such as these have been introduced with caution to preserve the integrity of the electoral process and maintain public confidence[13].

The goals of these changes were sound: increased accessibility, particularly to people with disabilities and non-English speaking populations, simplifying voting to protect against over-votes and other voter errors, improved accuracy, speed and reliability of results, and reduced staff costs. However, the inability of paperless electronic voting devices used in many jurisdictions to perform a meaningful recount resulted in ambiguous election results, which, in turn, led to a loss of public trust in elections[14].

Implementing Internet voting would require extensive revisions to long-established procedures for voting, counting, monitoring and auditing. It is critical that the general public trusts the security of new voting and counting processes and their ability to deliver a result that is a true and accurate reflection of their will as expressed through the voting process. If Internet voting is not trusted, voters may not accept the legitimacy of the elected members to govern. It is, therefore, very important that trade-offs among electoral principles are considered carefully.

This section assesses Internet voting with respect to seven principles of democratic elections. In so doing, it describes some of the challenges presented by Internet voting, trade-offs that may be needed among electoral principles, and best practices that have emerged from implementations of Internet voting in public elections.

1. Accessibility
2. Equal voting power
3. Secrecy
4. Security
5. Auditability
6. Transparency
7. Simplicity

[13] Recent events in the United States with the mass adoption of electronic voting machines following the 2000 presidential elections, serve as a vivid reminder of the consequences of changing voting and counting processes without adequate consideration of downstream effects.

[14] As an example, in a close race in Florida's 13th congressional district in 2006, 18,000 voters (14.9%) had no vote recorded for the congressional race by digital machines, although their votes for other races were recorded (New York Times, 2006). Without a paper trail, it has not been possible to adequately verify the result.

The Internet voting system descriptions presented in this discussion are based on systems in use elsewhere. They are used in this section as a backdrop against which issues raised can be compared and contrasted.

7.1 Accessibility

The principle of accessibility requires that voting opportunities are accessible to all eligible voters, regardless of their location, social status or abilities. The promise of Internet voting to enhance accessibility depends on the degree to which British Columbians have access to the Internet and ability to use it to vote. Accessibility also depends on the quality of the provincial voters list.

According to Statistics Canada (2010), British Columbians have among the highest rates of Internet use in Canada. Between 2007 and 2009, rates of personal Internet use increased in every province, with the highest rates reported in British Columbia and Alberta (both 85 percent). Use of the Internet is also growing rapidly; over the four-year period from 2005 to 2009, the proportion of British Columbians with access to the Internet rose from 69 to 85 percent. Internet use is particularly strong among younger Canadians, with almost all of those under 35 reporting use of the Internet in 2009.

7.1.1 Registered voters only

Depending on the approach taken, voters do not always have the opportunity to register in conjunction with Internet voting. Some implementations limit the service to voters who are registered prior to an established date so that, for instance, access codes can be sent via the post to eligible voters. In 2009, 92.5 percent of the 3.2 million eligible voters in B.C. were on the voters list. Just as younger voters are less likely to participate in elections, they are also less likely to register to vote. In 2009, for example, 69 percent of eligible voters under age 25 were on the list. Given current registration rates for young voters, it is possible that a relatively high proportion of one of the target populations for Internet voting will be ineligible to use the service if registration in conjunction with Internet voting is not permitted.

7.1.2 Digital divide

Because access to personal computers and the Internet is not equally distributed throughout the province and society, there are risks that Internet voting may highlight the “digital divide”. Figures from Statistics Canada suggest that, while a digital divide or gap in the rate of Internet use exists on the basis of income, education, age and community size, the gap narrowed between 2007 and 2009 for all categories except community size.

7.1.3 Technological and logistical barriers

Some of the accessibility gains of Internet voting may be off-set by standards that need to be met in the areas of authentication and security. Implementations of Internet voting that require voters to use non-standard equipment or to install specialized software will make the option less convenient to voters. As well, multi-step authentication processes may be necessary to confidently identify voters, but may also require advance planning on the part of voters that will make this channel less spontaneous than it otherwise would be.
To minimize risk to the principle of accessibility, the following ideas could be considered:

- Internet voting should not be considered as a sole channel for voting. By keeping other channels open, those who are not comfortable with, or cannot access, the technology, still have options to vote.
- The Internet voting interface should be user-friendly and the voting process as simple as possible.
- No special hardware or software should be required to participate in Internet voting.
- Public access to computers should be promoted (e.g. public libraries, Service BC offices, district electoral offices, etc.).

7.2 Equal voting power

The principle of equal voting power captures two important concepts: 1) only eligible voters can vote, and 2) each eligible voter can only vote once, thereby ensuring that each vote carries equal weight. To satisfy this principle, voters must be identified or authenticated prior to voting, and marked as having voting after their ballots are cast.

Authentication is a challenging area whether voting takes place in-person or remotely. The need to guard against impersonation and/or multiple voting must be considered along with the accessibility implications of the authentication system selected.

In an in-person setting, voters prove their identity and residential address to election officials by showing identification documents, or through a vouching process. Impersonation and multiple voting are possible in an in-person voting context if a voter has possession of someone else’s identification documents.

For postal voting, the standard of authentication is lower than in the voting place.

Voters provide their name and residential address at the time of application and sign a declaration, but no identification documents are required to be submitted with the voted ballots for pre-registered voters. Identification documents must be submitted with postal votes only for voters who are registering at the time of voting.

The same requirement to positively identify voters and to confirm their eligibility before allowing them to vote exists with Internet voting. In the absence of a comprehensive identity management system, several different authentication schemes have been developed. These usually involve multiple steps that make use of different communication channels to share PINs and personal information to assist with voter identification. To support this type of authentication process, it is important that the voters list has a high level of accuracy on attributes that might be used as shared secrets to positively identify a voter, such as date of birth.

Internet voting could be an additional channel, offered concurrently with other voting opportunities. When different voting opportunities occur at the same time, procedures need to be in place to ensure that only one vote per eligible voter is counted. Some implementations of Internet voting restrict its use to the advance voting period (e.g. Markham, Peterborough, Halifax and Geneva (Goodman et al., 2010)). As these approaches do not permit voters to vote again by paper ballot on voting day, it is likely that the voting list used in the administration of voting on that day reflects Internet voting activity to ensure against multiple voting.

It is also possible for an Internet voting option to remain available through to the close of in-person voting, while ensuring that only one vote is counted per voter. Some scenarios include:

1. Use of a real-time, electronic voters list throughout the network of voting places to allow election officials to ensure that voters have not previously voted.
2. Delaying the count of Internet votes to final count, as is currently done with absentee ballots.
3. Allowing voters to vote at multiple opportunities and having systems in place to ensure that only the last vote is counted.

7.3 Secrecy

There are two requirements for secrecy in a voting process. First, it must not be possible to associate a voted ballot with a voter. This requirement ensures that voters can express their true opinion, free from influence. The second requirement is that voters cannot be able to prove how they voted because this would open the door to coercion and vote buying and selling.

Maintaining secrecy is a challenge in the virtual environment because of the requirement to both authenticate the voter and to anonymize how the voter voted, while ensuring the integrity of the voted ballot management process. Conceptually, an Internet voting implementation could address the requirement for authentication and secrecy using encryption[15] based on industry standard cryptography processes. To use an analogy to postal voting, one should picture a two-envelope model (a voted ballot inside a secrecy envelope and the secrecy envelope inside a certification envelope bearing the voter's identity) where the seals on the envelopes are actually encryption around the voter's identification and vote.

Encryption and cryptographic methods are determined and implemented by system architects and software engineers with the goal that nobody but authorized election officials can open the seals and decode the voter's identity or the vote contents. To protect the secrecy of the vote, a system could be designed such that the secrecy envelope encryption cannot be opened while the certification envelope encryption is present.

In an in-person context, the voter's identity is separated from the contents of the vote when the ballot is deposited into the ballot box. In an Internet voting model, voters have to trust that election officials will sever the link between voter identities and their voted ballots and that these associations cannot be reconstructed by anyone.
In any remote voting context, the potential exists for voters to show others their marked ballot or to permit others to vote on their behalf. These risks may be part of postal voting, but exposure in an election is low due to the relatively small number of voters using this option (0.2 percent). The 2011 HST Referendum was conducted entirely by postal voting and its exposure to these risks is currently being reviewed.

The Estonian model of allowing voters to vote multiple times by different channels appears to be an effective means of dealing with vote buying and coercion. Giving voters this option means a second-party can never be certain how someone voted, and this reduces the potential for vote buying and selling schemes. However, this feature presents privacy issues as well. A link between the vote and the identity of the voter must be maintained and storing this link may be considered inappropriate (Schryen & Rich, 2009). In addition, it could be administratively challenging to ensure that only one vote is counted per voter when voters are permitted to vote multiple times by a mixture of electronic and in-person channels.

[15] Encryption is a process whereby plain text information is rendered unreadable by anyone other than those who possess the required code (sometimes called a key) to make the message readable again.

7.4 Security

The principle of security means that voted ballots are protected from tampering such that an election result is a true and accurate reflection of the choices made by eligible voters. Because Internet voting takes place in a distributed, non-transparent electronic environment that is not controlled by election officials, it raises the possibility for tampering on a much broader scale than more traditional types of voting. Use of the Internet to transport voted ballots introduces the potential for attacks on the voting system to come from anywhere in the world.

Although there has been no evidence of vote tampering or rigging in a public election using Internet voting, security experts warn that this does not mean that an attack has not occurred, or that it will not occur in the future. A well-executed attack may not be visible to voters or election officials (Jefferson, Rubin, Simons, & Wagner, 2004).

The potential far-reaching consequences of an attack were demonstrated in 2010, when the District of Columbia opened its Internet voting system to security testing. Within 36 hours of the system going live for testing, Alex Halderman, a computer scientist at the University of Michigan, gained access to the election server and took control of the system. Votes were modified and voters' identities were linked to their votes, violating secrecy. The attack went undetected by election officials for two business days (Zetter, 2010).

The literature is replete with various scenarios regarding how people with malicious intent could potentially subvert an election that uses Internet voting (see Geist, 2010, Jefferson, Rubin, Simons, & Wagner, 2004, or Rubin, 2001 for example).
It is important to recognize that the computer hardware and software used to deliver Internet voting is constantly being updated and patched as new vulnerabilities are identified and rectified. New modes of attack continually arise, so there is always the possibility of compromise.

The following section illustrate some of the main security issues related to Internet voting by following an example voting process from the voter's computer to election servers.

7.4.1 At the voter's computer

The most difficult link to protect in the end-to-end Internet voting process is the voter's computer or mobile device. Personal computers are often poorly maintained and not well protected from malware attacks (California Internet Voting Task Force, 2000). In a remote Internet voting context, the computers used to record and transmit votes are outside the control of the electoral agency and there is, therefore, not a lot that election officials can do to address these issues.

Operating systems and browsers are vulnerable to malware, which may be downloaded inadvertently by voters or others with access to the same device. Once inside a voter's computer or mobile device, malware could alter a voter's vote without the voter's knowledge, record voting activity, and display a voted ballot image that does not correspond to the data transmitted to election servers.

Voters would be able to detect irregularities if they had access to a trusted device or computer to review how their ballot was received. This is problematic, however, because allowing voters to confirm their vote might also allow them to prove how they voted. If tampering occurs prior to the voted ballot being sent, election officials may have no way to distinguish a reported discrepancy from user error, a change of heart, or a malicious change.

There are design features that can be implemented to minimize risks associated with the security of voters' personal computers. Ansper et al. discuss a remote electronic voting process that uses anonymous codes that are personalized to each voter (Ansper, Heiberg, Lipmaa, Overland, & van Laenen, 2011). These codes are distributed with voting cards (e.g. Where to Vote cards). One voter might be provided the code “234” to vote for the “White Party”, while another may be issued the code “135” for the same selection. This approach would make it more difficult for a malicious third party to interfere on a broad scale because the voting communication is different for each voter. Other options include the use of captchas, whereby voters select an image that most closely corresponds to their candidate of choice – e.g. to vote for candidate “A”, select the image representing a cat (Beaucamps, Reynaud-Plantey, Marion, & Filiol, 2009). Norway's planned distribution of vote verification codes through a variety of channels independent of the voter's personal computer (post and mobile phone) is another example of how reliance on the security of voters' personal computers can be reduced.

Providing verification codes and/or adding a human interpretation element to the ballot marking exercise increases security, but also makes the overall voting process more complicated and less accessible to those with low literacy levels. These approaches may also result in higher rates of voter error, thereby decreasing the overall accuracy of the election and the efficiency of electoral administration.

7.4.2 Communications infrastructure

Voted ballots travel from voters' computers or mobile devices to the election server via the Internet. Voters are vulnerable at this point to connecting to imposter sites, which may be indistinguishable from the real election site. There have been some significant improvements in the security features of web browsers, making it easier for people to confirm a secure connection (SSL) has been established with a trusted (certified) server. Access to this functionality depends on the voter being able to install the latest software and on having an uncompromised system with all known vulnerabilities patched.

Security issues in the communications portion of the journey relate to potential interruptions in service due to Denial of Service or DoS attacks. These attacks attempt to make the election server unavailable by overloading it with illegitimate service requests.

To mitigate against this type of attack the voting platform must be designed with sufficient contingency capacity to maintain service standards throughout the voting period. The issue in an election is that there may not be an opportunity to vote the next day, so it is critical that voting systems are available.

7.4.3 At the election servers

The election servers are the final, centralized gathering place of voted ballots. Election servers have to be Internet accessible in an Internet voting scheme to allow for voter authentication and the transmitting of voted ballots.   These servers have a relatively high potential for attack due to the quantity of sensitive material they store and must be protected with the highest standards of security available.

The integrity of an Internet voting system should be based on the design of the system and should not rely on the goodwill of those involved in its implementation (Schryen & Rich, 2009). In other words, the system should be designed in such a way that all known opportunities for malice are eliminated. An important area for consideration is the delegation of responsibilities related to the handling of voted ballot data received at election servers. Responsibilities must be delegated in a manner that a significant degree of trust is not vested in any one person.

Techniques need to be used throughout the server-side processing of voted ballots to protect against tampering. The system should be designed so that functions such as adding or altering votes cannot be performed. Sensitive operations, such as reading voted ballots and the removal of invalidated votes[16], need to be registered in protected logs that cannot be deleted or modified without detection.

However, even the most sophisticated security features can potentially be subverted by an insider with knowledge of and access to the system. One way to address this is to require two officials to collaborate to unlock the data (Puiggali, Choliz, & Guasch, 2010). This is analogous to procedures in the voting place that require two election officials to be present during the administration of voting and counting processes.

[16] For example, in the Estonian model, some Internet votes would be invalidated by in-person votes.

7.5 Auditability

The principle of auditability means that there must be an independent and documented means of publicly verifying and recounting votes to confirm the result of an election. This principle is central to public confidence because it means that whenever ambiguity arises regarding the count of votes, it can be addressed.

Electronic voting machines that do not provide an independent, voter verified means of audit have been widely criticized (Thompson, 2008). Remote Internet voting systems are similar in that they do not lend themselves to a voter-verified means of audit. In the context of Internet voting, verification of the accuracy of the result is achieved through two types of audit: auditing of votes and auditing of voting procedures and systems (Schryen & Rich, 2009). Each of these areas is reviewed below.

7.5.1 Auditing of votes

As only voters know how they actually voted and the security of ballots may be compromised prior to receipt at election servers, it follows that a system that facilitates voter confirmation that the vote was counted as cast is helpful to ensuring an accurate count. However, any process that involves sending information back to the voter regarding how they voted conflicts with the principle of secrecy. To confirm how a voter's vote was counted, the link between a voter's identity and their vote must be maintained, that information must be transmitted via the Internet, or some other channel, and exposed again to potential snooping. Upon receipt of proof of how they voted, voters could then show others how they voted.

Systems range in terms of the evidence provided to voters regarding what happened to their Internet vote. Voters may receive evidence that their vote was: a) received as cast, b) recorded as cast, and/or c) counted as cast.

The evidence provided to the voter (usually a type of code) must be in a format that cannot be reliably decoded by another person (Benaloh, 2008). In other words, voters cannot receive a plain text receipt of their vote because this would allow them to prove to others how they voted. To preserve voter privacy, electoral agencies must sever the linkage between votes and voter identity after distributing the encoded vote receipts.

In their 2006 House of Representatives elections, the Dutch used a system that provided voters with cryptographic proof that their votes were counted as cast and allowed voters to confirm the overall tally of votes. However, Schryen and Rich (2009) conclude the practical procedures to be followed by voters in that instance were so complicated that the system was considered dysfunctional. Any system of voter verification relies on voters to participate and must consider how discrepancies will be resolved.

It must also be recognized that, even when provided a record of their vote for verification, voters in a remote Internet context will always be dealing with a representation of their vote, rather than the actual vote itself, which exists only in electronic form. Voters would have to trust that their receipt is a true representation of their electronic vote.

A means of verifying the accuracy of voted ballots arriving at election servers without involving voters would be to test the system during operation. For example, a series of test ballots from computers established throughout the province could be sent to election servers during the election. The particulars of these ballots (number, location, timing, contents) would be known by the election server, but they would otherwise be indistinguishable from regular voted ballots.

7.5.2 Auditing of voting procedures and systems

Voting systems need to be evaluated, tested and certified to demonstrate the absence of known issues and that software code functions as intended. These auditing processes should be conducted by independent experts with the necessary expertise.

Secure log files that track system events should be produced and reviewed to confirm the integrity of the vote management processes.

7.6 Transparency/simplicity

Transparency refers to the openness with which decisions, actions and voting and counting processes are carried out. It is a critical piece to ensuring public confidence and trust in election outcomes. Simplicity refers to the ease with which voters can participate in and observe the system, and the ease of administration. The principles of transparency and simplicity are different, but are addressed together in this section because they are closely related. Processes that are simple for voters to use and understand also tend to be highly transparent and vice versa.

Perhaps the greatest strength of paper-based voting systems is their transparency. These are relatively simple processes taking place in the physical world that are readily observed and understood. Purely electronic systems cannot offer the same level of transparency and simplicity. The nature of computers is such that their inner workings are impenetrable to anyone who is not an expert (i.e., black box effect).

In the context of Internet voting, members of the voting public are not able to ensure that systems are working as intended and they must rely on independent experts to do this on their behalf. Scrutineers observing the management of voted ballots and the count of Internet votes also require specialized knowledge to be effective in their role.

To ensure public confidence in results generated by an Internet voting system, electoral agencies, software designers, and system architects need to build systems and procedures with transparency, openness and simplicity in mind. To the greatest extent possible, the design, testing and implementation of an Internet voting system and overall election procedures should be made available for public review. The findings of audits conducted by independent security experts should be made public as well.

7.7 Summary

Internet voting presents a challenge to policy makers. On the positive side, Internet voting fits with the B.C. government policy direction to provide citizens with access to a greater variety of high quality online services.

Internet voting offers voters a convenient alternative to in-person voting. This may be particularly important to voters who have difficulty attending in-person voting opportunities. And finally, concerns about the digital divide are diminishing as the proportion of British Columbians who use the Internet continues to grow.

Policy makers need to weigh these positive considerations with compromises that Internet voting would entail for several foundational principles of elections. With the current state of technology, Internet voting is considered to be less effective than traditional, in-person and postal voting methods at protecting ballots against large-scale fraud, ensuring the secrecy of the vote, and providing a fully transparent and observable process that can be effectively audited. Because specialized computer skills are required to observe an Internet voting process, voters would have to delegate their trust to "experts" to confirm that the election is conducted properly.

8.0 Internet voting in B.C. provincial elections

As mentioned in the introduction, it is not currently the policy of the BC Government to offer Internet voting in provincial elections. The province's *Election Act* is based on a conceptual framework of physical voting places under the direct control of election officials.

Under section 281 of the *Election Act*, the Chief Electoral Officer has broad powers to trial new election procedures in the context of a by-election with the approval of the Election Advisory Committee. However, any new procedures would have to be implemented within the current framework of physical voting places. The *Election Act* would have to be amended for Internet voting to be trialed in a provincial event.

The development of public policy around Internet voting needs to address a number of issues raised in this paper. For example, if Internet voting was to be offered, would it be available to everyone, or would it be limited to specific groups or in defined circumstances?

Various countries in Europe have chosen different paths, reflecting their own values. Germany, for instance, has taken the stance that no compromise in principles is acceptable and voting must be completely transparent. Estonia and Switzerland, by contrast, do not restrict access to Internet voting. The Netherlands and Australia occupy the middle ground, recognizing a role for technology in meeting the particular accessibility needs of citizens who reside overseas and people with disabilities.

Other questions for policy makers include:

- How can transparency and verification be built into an Internet voting system to ensure public trust in outcomes?
- Would Internet voting be an additional channel layered on top of existing opportunities; would it replace one or more existing voting opportunities?
- When during the election period would Internet voting be made available?
- What would happen if fraud was detected on a large scale?
- How would the system guard against multiple voting across various voting opportunities?
- How would the system be structured to ensure separation between voter identity and voted ballots?
- What methods would be used to provide end-to-end verifiability without sacrificing voter privacy?
- How would an Internet voting system be observed?
- How would the system be independently audited?

8.1 Summary

Voting and counting processes vary from jurisdiction to jurisdiction reflecting the particular trade-offs made by policy makers regarding the principles of free and fair elections. The goal of most modern voting systems is to maximize accessibility and convenience, while safeguarding the other principles of free and fair elections to an extent that ensures public confidence in the outcome. Each jurisdiction arrives at its own trade-offs reflecting local culture, the values and skills of constituents, and available technology and resources. As pressure grows to modernize B.C.'s voting process, it is important that policy makers maintain a steady focus on the need to maintain public confidence in the voting process and that change strikes a balance among electoral principles that is acceptable to British Columbians.

9.0 Bibliography

Alootechie. (2011, May 24). Gandhinagar Municipal Corporation uses internet voting technology for conducting elections. Retrieved from http://www.alootechie.com/news/gandhinagar-municipal-corporation-used-internet-voting-technology-conducting-elections

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

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

Barnes, E. (2010, November 1). Internet Voting Arrives...But is it Secret and Secure. Retrieved from http://www.foxnews.com/scitech/2010/11/01/internet-voting-secret-safe/

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

Benaloh, J. (2008, July). Ensure Election Accuracy. Tech-Net Magazine. Retrieved from http://technet.microsoft.com/en-us/magazine/2008.07.fieldnotes.aspx

Bochsler, D. (2010). 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.

California Internet Voting Task Force. (2000, January 18). Technical Committee Recommendations. Retrieved from: http://sos.ca.gov/elections/ivote/appendix_a5.htm

Canadian Council of Better Business Bureaus. (2010). Consumer Tips: Identity Theft. Retrieved from: http://mbc.app.bbb.org/tips?id=104

Chowdhury, M. J. (2010, September 6). Comparison of e-voting schemes: Estonian and Norwegian solutions. Retrieved from: http://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-draft.pdf

EKOS. (2009, December 17). To Vote...Click Here: Canadians want Internet voting in federal elections. Retrieved from: http://www.ekos.com/admin/articles/cbc-2009-12-18.pdf

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

Elections BC. (2010). Report of the Chief Electoral Officer on the 39th Provincial General Election and Referendum on Electoral Reform - May 12, 2009. Victoria: Elections BC.

Elections Canada. (2011). Report of the Chief Electoral Officer on the 41st General Election of May 2, 2011. Ottawa: Elections Canada.

Estonian Bureau of Citizen and Immigration. (2011, 06 01). Information box at top left. Retrieved June 1, 2011, from www.id.ee: http://www.id.ee/

European Parliament. (2011, 03 23). Can e-voting increase electoral participation? Retrieved from: http://www.europarl.europa.eu/en/headlines/content/20110321STO15986/html/Can-e-voting-increase-electoral-participation

Federal Constitutional Court. (2009, March 3). Use of voting computers in 2005 Bundestag election unconstitutional. Retrieved from: http://www.bundesverfassungsgericht.de/en/press/bvg09-019en.html

Geist, M. (2010, March 10). Casting a Vote Against Internet Voting. Retrieved from: http://www.michaelgeist.ca/content/view/4856/135/

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

Internet Policy Institute. (2001). Report of the National Workshop on Internet Voting: Issues and Research Agenda. Internet Policy Institute.

Ivens, A. (2011, January 12). Online voting would boost participation in elections: Christy Clark. Retrieved from: http://www.theprovince.com/news/Online+voting+would+boost+participation+elections+Christy+Clark/4100624/story.html

Jefferson, D. (2011, February 10). Dangers of Internet Voting and Solutions for Overseas Voters. OVF Conference . Washington, D.C., USA: Verified Voting and Lawrence Livermore National Laboratory.

Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004). A Security Analysis of the Secure Registration and Voting Experiement (SERVE).

Joint Standing Committee on Electoral Matters. (2009, March 16). Report of the 2007 fedral election electronic voting trials. Retrieved from: http://www.aph.gov.au/house/committee/em/elect07/report.htm

Krebs, B. (2008, February 20). Banks: Losses From Computer Intrusions Up in 2007. Retrieved from: http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html

Kripp, M. (2011, March 14). Internet voting in Estonia - Internet voting is necessary to maintain turnout and integrate voters. Retrieved from: http://www.e-voting.cc/stories/14871513/

Nestas, L. H. (2010). Building Trust in Remote Internet Voting. Bergen: University of Bergen, Department of Informatics.

Nore, H. (2010). Open Source Remote Electronic Voting in Norway. Vienna: The Ministry of Local and Regional Development.

Puiggali, J., Choliz, J., & Guasch, S. (2010, August 3). Best Practices in Internet Voting. Retrieved from: http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PUIGGALI_BestPracticesInternetVoting.pdf

Rubin, A. D. (2002). Security Considerations for Remote Electronic Voting. Communications of the ACM , 45 (12), 39-44.

Schneier, B. (2001, February 15). Internet Voting vs. Large Value e-Commerce. Retrieved from: http://www.schneier.com/crypto-gram-0102.html#10

Schryen, G., & Rich, E. (2009, July 17). Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland. Retrieved from: http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20Rich%20-%20Security%20in%20Large-Scale%20Internet%20Elections%20-%20IEEE%20Transactions.pdf

Statistics Canada. (2010, May 10). The Daily: Canadian Internet Use Survey. Retrieved from: http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-eng.htm

The Electoral Commission. (2007). Key Issues and Conclusions: May 2007 electoral pilot schemes. London: The Electoral Commission.

Thompson, C. (2008, 6 January). Can You Count on Voting Machines? New York Times , pp. http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html

Unique Identification Authority of India. (2011). Background. Retrieved from: http://uidai.gov.in/index.php?option=com_content&view=article&id=141&Itemid=164

Verified Voting. (2011, May 23). Internet Voting in India? Gujarat is the Early Adopter. Retrieved from: http://thevotingnews.com/international/asia/india/internet-voting-in-india-gujarat-is-the-early-adopter-plugged-in/

Zetter, K. (2010, October 6). Hacked Voting System Stored Accessible Password, Encryption Key. Retrieved from: http://www.wired.com/threatlevel/2010/10/voting-system-hacked/

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

ELECTIONS BC
A non-partisan Office of the Legislature

(11/08)