Research Study

ESTABLISHING A LEGAL FRAMEWORK FOR E-VOTING IN CANADA

Prepared for Elections Canada by
Dr. Bryan Schwartz
Professor of Law
University of Manitoba
and
Dan Grice, J.D.,
University of Manitoba

September 2013

Elections Canada

Table of Contents

NOTE TO READER

This paper was prepared by Dr. Bryan Schwartz, Professor, Faculty of Law, University of Manitoba and Dan Grice, J.D., University of Manitoba, for Elections Canada. The observations and conclusions are those of the authors and do not necessarily reflect the opinions of Elections Canada.

Establishing a Legal Framework for E-voting

Canadians have a constitutional right to vote that requires the government to make reasonable efforts to facilitate their ability to exercise their franchise. Even before the adoption of the *Canadian Charter of Rights and Freedoms*, Canada's legal framework for voting had been constantly evolving to increase access to voting.

One of the ways that has been discussed to increase access to the electoral system is to allow Canadians to cast a vote using a computer, either from home over the Internet or in a controlled environment, such as a voting kiosk in a designated polling area. This is commonly referred to as e-voting, and is slowly being adopted for local, regional and national elections in jurisdictions around the world.

E-voting can serve as an alternative means of voting in addition to in-person, mail-in and advanced voting. The electoral authority would administer it, and it could either be limited to voters who have difficulty getting to the polls (such as disabled or absentee voters) or available to all eligible Canadians.

The authors of this paper acknowledge that there are legitimate concerns with how e-voting would work and whether technological problems or malicious acts could pose a serious threat to the integrity of an election. We are also keenly aware that our democratic system requires voters to have confidence in the voting process.

This paper was commissioned by Canada's electoral authority, Elections Canada. Elections Canada is an independent, non-partisan agency that reports directly to Parliament. As part of its mandate, it must be prepared at all times to conduct a federal general election, by-election or referendum. It is also responsible to administer the political financing provisions of the *Canada Elections Act*, monitor compliance and enforce electoral legislation.

Elections Canada is also mandated to conduct voter education and information programs, and provide support to the independent boundaries commissions in charge of adjusting the boundaries of federal electoral districts following each decennial census. Finally, Elections Canada may carry out studies on alternative voting methods and, with the approval of parliamentarians, test electronic voting processes for future use during electoral events.

The goal of this paper is to recommend a legal framework for e-voting in Canadian federal electoral events. The research consisted of conducting extensive case studies of other jurisdictions' legal frameworks and experiences, which were then synthesized to present the most pertinent details. Based on this literature review, we present our findings and recommendations on what should be included in a Canadian framework.

The goal of this paper is not to advocate for or against e-voting, but rather to identify what issues a legal framework should address to minimize the risks associated with e-voting and ensure that Canadians can have confidence in the process.

At the minimum, e-voting should be as secure and reliable as special balloting currently conducted by mail. Ideally, it should also meet the following attributes and values that Canadians currently have under the paper-based system:

- facilitated accessibility and reasonable accommodation
- voter anonymity
- fairness
- accurate and prompt results
- comprehensible and transparent processes
- system security and risk assessment

- detection of problems and remedial contingencies
- legislative certainty and finality
- effective and independent oversight
- cost justification and efficiency

None of these values are absolute, and even the constitutional right to vote may be reasonably limited or rely on trade-offs among conflicting values.

In order to recommend a comprehensive legal framework, this paper looks at the legislation, regulations and procedures that have been developed to introduce e-voting at a national level in Estonia, a regional level in Australia and Switzerland, and a municipal level in Norway and even Canada, to determine best practices. We have supplemented this with observations and reports from international organizations and reputable election observers, including the Council of Europe, Organization for Security and Co-operation in Europe, the International Foundation for Electoral Systems and The Carter Center, along with academic works.

The ideal legal framework appears to be one that demands broad consultation and contemplates risks, problems and threats. It will require strong security measures and testing, but will also outline clear steps to take if worst-case scenarios occur. It will offer clear legislative standards, while allowing the electoral authority considerable flexibility to adopt the most advanced technology.

The legal framework for an e-voting test project or widespread use in a Canadian federal election could take one of a variety of formats. Standards, rules and other normative requirements may be contained in new or amended legislation (particularly the *Canada Elections Act*), subordinate regulations or direction by Elections Canada contained in policy statements, manuals, requests for proposals and other contractual documents. However, if e-voting is used in a general election, the stakes will be higher and more processes ought to be implemented to ensure that the effective right to vote is not displaced.

Ultimately, whether we use paper or computers to vote, the goal should be to ensure as many Canadians vote as possible, while providing the public confidence that the voting process will perform as Canada's democratic tradition requires.

Main Findings and Recommendations

In considering a legal framework for e-voting in a federal election, the recommendations made in this paper take into account operational elements that are critical in ensuring the implementation of such systems.

Format of the Legal Framework

The legal framework should be a combination of legislation approved by Parliament as well as regulations, policy statements and documents issued by the electoral authority. The framework should achieve legislative certainty while ensuring that adoption of new technology is not hindered by a slow legislative process. Ideally, minimum standards and basic requirements should be listed in legislation, while the electoral authority should be given flexibility to create transparent regulations and public policy documents.

Access and Eligibility

E-voting can be introduced to facilitate accessibility and provide reasonable accommodation to voters who have difficulty attending traditional voting, or it could be expanded to allow all voters to use e-voting. These decisions may involve accommodating cost effectiveness, efficiency, voter fairness and even risk assessment. The legislative framework should treat e-voting as the functional equivalent of special ballots conducted by mail, and non-electronic alternatives should always be accessible. While electronic ballots may be analogous to paper, the constitutionally guaranteed effective right to vote likely demands that voters who do not trust or feel

comfortable using computing technology are provided with sufficient options and feel confidence that their vote is secure. We recommend:

1. E-voting should be treated as the functional equivalent to special or postal ballots and non-electronic alternatives should always be accessible.
2. If there is a desire to limit electronic voting to a specified group, the *Canada Elections Act* should clearly prescribe the eligibility requirements. (Some jurisdictions only allow out-of-district voters, disabled voters and those who live a fixed distance away from the polls to vote over the Internet.)
3. Access to electronic voting should be broad enough to ensure that implementation costs are not overly disproportionate to traditional voting.
4. Parliament should grant the electoral authority flexibility in choosing the methods of authenticating voters as long as the methods are secure and reliable.
5. Electoral officials should work with diplomatic officials to determine which countries are safe to allow remote voting in.
6. The period for e-voting should be conducted over at least a week and end no earlier than the close of advance polls but before voting day. The period should be fair to e-voters but also allow the electoral authority time to react to technical problems.

Transparency

Public confidence in e-voting will depend on comprehension and transparency. The legal framework should ensure the public has access to information about the system's integrity and security, and methods should be in place to allow key stakeholders to independently verify the security and integrity of the system.

While the implementation of electronic voting in some jurisdictions has required all e-voting source programming code to be published online or to use only open source code, we recognize there may be valid reasons for allowing suppliers to protect trade secrets and for giving the electoral authority the flexibility to choose the most secure and reliable technology. Current legislation allows candidates' representatives to monitor all critical steps of voting. Similar steps should be taken with e-voting to ensure transparency. We recommend:

1. Party- or candidate-appointed scrutineers should be able to view all source programming code and inspect physical technology.
2. A formalized process should be created for academics and international observers to get similar access to ensure the integrity of the e-voting system.
3. Decisions on whether to publicly post source code or use open source technology should not be legislated, but should be left up to electoral officials.
4. Electoral officials should be required to provide public reports on the security and integrity of the e-voting system, as well as which external reviewers approve the system.
5. Legislation or regulations should ensure that observers or developers immediately report errors to election authorities.
6. Procedures should be in place to have election officials inform key stakeholders, including political parties, of security incidents.

Division of Roles and Responsibilities in Administering E-voting

A successful implementation of e-voting will require well-defined roles and responsibilities to ensure the system is secure and to provide the public with confidence that any negligence or mischief at the electoral authority cannot affect the accuracy of the votes or voter anonymity. The legislative framework should ensure that e-voting does not overly depend on any one individual or closely connected group. We recommend:

1. Some independent group with recognized technical expertise, internal to Elections Canada or external, should be required to certify and approve that a system is secure, reliable and ready to be deployed in a general election.
2. Roles should be assigned to determine if an electronic voting system's security, integrity or privacy has been breached.
3. Cryptographic keys should be divided among enough individuals, ideally representing different political parties, to protect voters' privacy and ensure votes are not prematurely de-encrypted.
4. A general division of technical roles and duties should be in place across the electoral authority to counter concerns regarding centralization and collusion and to ensure that at least two unconnected people approve any changes.

Contingency Planning for Worst-Case Scenarios

The *Canada Elections Act* contains some remedial language for reacting to worst-case scenarios, such as allowing the Chief Electoral Officer to adapt the Act in response to an "emergency, an unusual or unforeseen circumstance, or an error" (s. 17. (1)) and permitting a judge to order a revote. Confidence in the e-voting legal framework will be increased if remedial contingencies for known electronic risks are included in legislation and clear disaster plans are implemented to detect and react to problems. The legal framework should ensure legislative certainty and finality of the results. We recommend:

1. Clear procedures should be created, preferably in the *Canada Elections Act*, for cancelling electronic voting, notifying voters and allowing recasting of votes if privacy, security or integrity has been unacceptably compromised.
2. The Act should list conditions under which officials may temporarily expand the online voting period if service is interrupted for more than a determined time.
3. Requirements in the Act and regulations should be in place on how to treat invalid votes and other irregularities.
4. Regulations should detail how electronic votes are handled during a recount, although we recommend that the Act provide judges with increased discretion as to whether e-votes should be recounted in the case of a close election result.
5. A clear disaster recovery plan covering all known risks of disruption should be produced before each election.
6. The government should ensure that a technical response team, including leading Internet service providers, other departments, and anti-virus and securities vendors, is formed to identify and respond to potential threats during an election.

Electoral Offences

The *Canada Elections Act* contains a list of offences, cast in general terms, that may not be sufficiently broad or clear with respect to conduct that specifically concerns e-voting. In order to ensure legislative certainty and discourage disruptions to the electoral system, legislation should be passed to forbid attempts to abuse e-voting. Additionally, the potential for creating widespread voter fraud affecting multiple electoral districts should be taken into consideration in determining appropriate sentences or fines. We recommend:

1. Fines and penalties associated with voting offences, including influencing the vote, should be increased.
2. The *Canada Elections Act* should make it an offence for all technical support staff, vendors and anyone who may have access to the system to violate the secrecy of the vote.
3. Employers (and others) who use screen capture technology or other methods to observe their computers should be required to take reasonable steps to ensure the secrecy of the vote, including alerting employees.

4. Stiff penalties and specific offences should be created for attempts to systematically affect the vote, including disrupting election servers, manufacturing vote-altering software and interfering unlawfully with any electronic voting equipment.
5. The Act should ban wilful creation, promotion and linking to spoof election sites that could lead someone to wrongly think that they have voted.
6. The Act should make it an offence to wilfully corrupt and submit an e-vote.
7. Legislation should prevent unauthorized disclosure of e-voting source programming code.

Technological Standards and Consultation

The legal framework for e-voting should give the electoral authority a high degree of flexibility to choose the most secure technology, work on cost-effective solutions and deliver accurate results. Legislation should generally be permissive to allow new technology as long as it is secure, accurate and protects voter anonymity. A consultative process may be set up to ensure that the best technology is chosen. However, the choice of technology may also depend on certain functionality and features that may require trade-offs, such as between transparency and absolute secrecy. In those circumstances, legislative amendments and parliamentary discussion may be required. We recommend:

1. A transparent consultation process should be in place before technological standards or requests for proposals are formalized.
2. Parliament should discuss allowing voters to update or recast their e-ballot.
3. Officials should be permitted to introduce additional technology, including voter receipts or advanced authentication methods, if they are satisfied that it will increase integrity without disproportionally affecting the privacy of the voter.
4. Voters should be permitted to cast a blank ballot.

Testing and the Integrity of the Vote

To ensure the votes are accurate and the e-voting system is secure, the legal framework should require extensive testing at all stages and specific security steps. Ideally, minimum requirements would be in legislation and the electoral authority would be tasked to create detailed regulations and procedures. We recommend:

1. Regulations should clearly describe the tests that ought to be conducted prior to e-voting deployment.
2. Tests of the software should be completed to ensure it is accessible and usable. Disabled voters, seniors and other groups should be involved in the testing.
3. Regulations should require that physical security measures be in place to ensure the integrity of all equipment and prevent unauthorized access during an election.
4. Legislation should require auditable and unalterable records of voting activity, threats, disruptions and system activity. The electoral authority could create procedures that include unalterable tape backup and cryptographic encryption of logs.
5. Sufficient auditing procedures should be required post-election, even if some details of the audits remain confidential.
6. Procedures and timelines should be prescribed for destroying all voting data once all appeals are exhausted.

Controlled E-voting

The electoral authority may seek to deploy e-voting in a controlled environment to facilitate accessibility and accommodate more voters. These may be stand-alone e-voting devices used for voters requiring assistance or secure Internet connected systems running the standard e-voting software used by remote voters in an uncontrolled environment. We recommend:

1. Legislation should permit electoral authorities to host controlled e-voting for military voters; voters in penitentiaries; overseas voters at embassies, high commissions and consulates; domestic voters in locations such as offices of the returning officer; disabled voters in the home; and voters on post-secondary campuses, where absentee ballots are common.
2. Regulations should require e-voting devices to be tested before and after elections.
3. The electoral authority should have access to all software and code installed on machines.

Further Consideration: Specialized Oversight of E-voting

The centralized and technical nature of e-voting requires effective and independent oversight. Public confidence in the system will be enhanced if those overseeing the electronic voting system have the technical expertise, independence, reliability and multiparty support to make tough decisions related to e-voting. Further discussion is required to determine whether this would be most effective within the electoral authority or with a new body with independent powers. We recommend that the electoral authority and those representing various political parties work together to create a board or committee with the authority to make recommendations to the electoral authority or arrive at certain determinations regarding e-voting oversight. Potential members include:

1. federal court judges or others with positional independence
2. tenured academics specializing in engineering, computer science or law
3. privacy or information commissioners
4. others recommended by various political parties

2.0 INTRODUCTION

Scope

"Clearly, in a democratic society, the right to vote as expressed in s. 3 must be given a content commensurate with those values embodied in a democratic state" (*Haig v. Canada*, 1031).

Since the introduction of the secret ballot in Canada in 1874, arguably little has changed with the actual act of voting that involved a voter marking a symbol next to the candidate whom they wish to represent them in Parliament.

This is not to say that election regulations and legislations themselves have remained stationary. Electoral legislation has been changed to extend the franchise to women and other groups, lower the voting age, include party names on ballots, allow voters to register at the polls in rural and then urban areas, provide additional voting days and accommodate disabilities. Some of these were part of global trends, while others were uniquely Canadian decisions either spurred on by the electorate, or in some cases, such as prisoner voting, mandated by the courts based on Charter rights.

The push for Internet voting and other electoral technology (collectively called electronic voting or e-voting) is arguably a continuation of attempts to make elections more accessible. Instantaneous interaction with centralized computers has the potential to facilitate voting from home or abroad, and allows electoral officials to consider alternative methods of casting votes and transmitting them to the electoral authority. In an online system, a voter should be able to securely and privately visit a website, enter a user identification number and password, and cast a ballot.

Any change in how Canadians vote will require a comprehensive legal framework. The main purpose of this paper is to provide assessment to electoral decision makers in Canada considering implementing remote Internet voting in some capacity in a future federal election. This paper also references other electronic technology used in a controlled setting, albeit in a limited way.

The goal of this paper is to recommend a legal framework for e-voting in Canadian federal electoral events. This paper was commissioned by Canada's electoral authority, Elections Canada, an independent, non-partisan agency that reports directly to Parliament. Its mandate includes conducting federal electoral events and administering the *Canada Elections Act*, which would be a critical component of an e-voting legal framework.

Our research consisted of conducting extensive case studies of other jurisdictions' legal frameworks and experiences, which were then synthesized to include the most pertinent details. The legal framework for e-voting will span various legal and institutional instruments, including legislation, regulations and policies.

The goal of this paper is not to advocate the benefits or underestimate the risks of e-voting, but rather to present options for regulations and legislation that could mitigate and manage the risks and increase voter trust in a new system. Where possible, this paper recommends ways to make e-voting as secure and accurate as current means of voting.

Canada is not alone in exploring the use of Internet voting. Other countries, including Estonia, Switzerland, Norway, Australia and France, have already begun testing it at various levels of government, as well as developing regulations and legislation for its implementation. Even within our borders, a number of municipalities and political parties have experimented with Internet voting, and several provinces are also exploring the potential.

Methodology

Our research consisted of reviews of academic and stakeholder commentary, observer reports from the conduct of elections and auditor reports, as well as a close look at naysayers and groups who remain suspicious of the risks of election results. Where regulations and legislation existed, this paper compares them with what currently exists in Canada. This paper is not limited to the circumstances surrounding Internet voting alone, but also reviews other uses of technology in the voting process, to look at how best practices under different contexts have been used.

Much can be learned about the legal framework and practical results of Internet voting taking a comparative law approach.

Law reform in Canada often involves studying laws that have been enacted and implemented in other countries, and adapting and adopting them. There are many advantages to this approach. Comparative exercises help to identify new policy concepts. They can provide a framework for thinking through the merits and demerits of various options. The text of legislation in other jurisdictions can provide inspiration and guidance on how to translate concepts into legal language.

Legislation in other jurisdictions can provide indispensable lessons for Canadian policy makers. Many apparently promising legal ideas turn out to have unexpected and adverse consequences. The subjects of legislation may find surprising ways to avoid or overcome their strictures. There can be no laboratory experiments in public policy making; the only way to test ideas is through societal practice.

Sceptics of Internet voting, however, might argue that comparative exercises must be viewed with caution. There is the risk in comparative exercises that "a little knowledge is a dangerous thing." An observer might focus on a particular law without appreciating the larger legal context in which it occurs. For example, it is true that Estonia has used Internet voting, but it must be recognized that its voting system is proportional representation, not like Canada's first-past-the-post system (where the candidate with the most votes wins). The difference of a few votes, or even a few dozen votes, might not have a substantial impact on the outcome of an Estonian

election; seats are allocated on the basis of a percentage of votes achieved throughout the entire country. On the other hand, in a plurality system such as used by Canada, a single vote in a single constituency could determine the balance of power in the House of Commons.[1]

As another example of how Canadian elections can be closely contested, in the 2011 federal election, 5 seats were decided by fewer than 100 votes (Funke, n.d). In highly contested votes, it is foreseeable that the number of electronic voters would in many constituencies exceed the margin of victory from traditional balloting. The practical implications of e-voting would intensify the need to ensure that instructions to voters and accessibility and reliability of the technology are intrinsically sound and adequately explained to the public.

Similarly, in examining the Estonian experience, one might overlook that part of its success is due to its reliance on the existence of a national identity card, for which there is no counterpart in Canada. Another risk in comparative exercises can be a misguided belief that the "law on the books" is the law in reality. The official legal code, for example, might be selectively enforced or not at all.

There is also the risk of overlooking the geographical, social or economic differences between the countries compared. One particular risk in the Canadian context is overlooking the issue of scale. A system that might work in a geographically and demographically small jurisdiction might run into unexpected difficulties if extended, without careful thought, to a much larger one. Currently, there is limited use of Internet voting at a national or even state level in a major election. The four most predominant deployments so far have been in Estonia at the national level, with a population about the size of Manitoba; France, where 240,000 overseas votes were cast; (Scytl 2012) and Switzerland, which limits e-voting to 10 percent of its voters. Only Australia's New South Wales state, which is roughly the size of Quebec, is closely analogous to Canada in using online voting in a parliamentary election. However, the state printed each Internet vote and manually counted the 44,000 votes cast online across 93 legislative districts. Additionally, Internet voting was limited to distance and disabled voters (Brightwell 2011).

In conducting the comparative part of this study, special emphasis was placed on jurisdictions such as Norway and Estonia, where there is extensive access to the legal standards used, and on reports on how e-voting actually worked in practice. We also drew on European as well as domestic sources of law and guidance.

This study has attempted to keep in mind as well that when the stakes are higher, as in national-level elections, there might be much greater incentive for misconduct.

The ability to alter the balance of party power in Parliament might be a big enough prize to attract earnest tampering efforts by persons motivated by commercial or ideological interests to affect the results of an election. Additionally, it may also attract those with no direct interest in the results of an election, but who want to disrupt the election.

The advantage of our methodology of extensively setting out principles, standards and procedures include the following:

- The discipline of formally and publicly documenting guiding norms will encourage more precision in thinking through the real-world application of those norms.
- The existence of a well-documented set of guiding norms will assist parliamentarians in evaluating a proposed test of Internet voting and facilitate public input into that process and the promotion of public trust in the process.

[1] For example, in Canada, a 2005 non-confidence motion was decided by a single vote in Parliament. If that Member of Parliament had been elected by one vote, then the vote in the constituency would have effectively determined the outcome of that motion.

- The documentation will facilitate the eventual legislation of changes to the *Canada Elections Act* or its accompanying regulations should Parliament wish to continue testing Internet voting or to adopt it as an integral part of the national voting system.

There are limits, however, to how much can or should be placed in a set of guiding norms. Some discretion is likely desirable to select among different technical options, including the hardware for receiving and tabulating votes and outside experts to test and certify systems, and to react to problems as they arise.

Structure of This Paper

This paper contains two major parts: "Background, Context and Literature Review" and "Main Findings and Recommendations."

The first part contains an overview of how e-voting is used in both an uncontrolled environment and a controlled environment. This part provides a brief overview of both the benefits and concerns raised with introducing e-voting. This is followed by an overview of Canada's constitutional right to vote and an introduction to the notion of functional equivalence, which requires synthesizing key attributes from the current legislation and applying them to e-voting so that the e-voting rules function in an equivalent way to paper-based voting. Next, there is a summary of the experiences in other jurisdictions with e-voting as well as a brief overview of some of the major international organizations that have conducted work on e-voting. The major findings of these groups are also summarized as an appendix. Lastly, there is a summary of the key values and attributes that are important to conducting elections, whether by computer or paper.

The second part surveys specific components of legal frameworks for e-voting and makes recommendations on what should be included in a Canadian framework. This is introduced by a brief discussion about the form of the framework, such as comparing legislation passed by Parliament with regulations and policy issued by an electoral authority. The discussion and recommendations are grouped into nine topics:

1. When are voters eligible and under what circumstances can they access e-voting?
2. What measures are taken to ensure the e-voting system is transparent?
3. What major roles and responsibilities are required to administer e-voting?
4. What contingency plans should be in place for worst-case scenarios?
5. What electoral offences should be created for e-voting?
6. What technological standards and consultation are needed?
7. What types of testing are needed to ensure the integrity of the vote?
8. What unique considerations are required for controlled voting?
9. Is there a need to restructure the electoral authority?

3.0 Background, Context and Literature Review

This paper explores legislative issues related to alternative voting methods in both controlled as well as uncontrolled voting over the Internet. An example of a controlled voting environment would be a stand-alone voting kiosk (not connected to the Internet) run by election officials at a specially designated polling area. Uncontrolled e-voting is essentially voting by a home or public computer using an Internet browser or a specialized application that securely transmits a ballot over the Internet.

In developing a legal framework for e-voting, one should be aware of how different types of e-voting work, what constitutional requirements may exist in Canada, what other jurisdictions experiences are with e-voting and what international guidelines currently exist. The following is a summary of some the background work that was used to formulate this paper's recommendations.

E-voting in an Uncontrolled Environment (Internet Voting)

Mechanics of E-voting in an Uncontrolled Environment

An uncontrolled environment includes the home, where a voter uses a personal computer to cast a ballot that is transmitted electronically to a server operated by the government.[2] Similar to mail-in ballots, in an uncontrolled environment, there is no way to ensure that a voter's privacy is not compromised, potentially facilitating bribery or intimidation. Unlike with controlled voting, election officials do not have the ability to test the voting device (the user's computer), potentially increasing the risk that malware or a virus could manipulate voters undetected. These programs could alter individual votes or falsely indicate that their vote had been uploaded to a server (Beaucamps et al. 2009). Similarly, there are worries that counterfeit websites or fraudulent emails may mislead less technically savvy voters into thinking they had casted a vote (Geist 2010).

With Internet voting, the voting software is installed on a server or across multiple servers at secure locations, and voters cast their ballot either by downloading a secure voting application from the elections administrators' website, which then sends an encrypted vote over the Internet, or by logging directly into a secure web portal to vote. Also, some vendors may provide applications that can run on smart phones and tablet computers. Uncontrolled systems are often used as an alternative to postal voting, allowing voters who will be outside a voting area or more than a certain distance from a polling station to cast a ballot from any location. By automating counting and avoiding having to rely on international postal services, electronic voting can reduce the logistics in enfranchising voters (Goldsmith 2011). For instance, France allowed all citizens who lived overseas to vote online in its 2012 parliamentary election. Some jurisdictions, such as the Australian state of New South Wales, have implemented this system to assist individuals with disabilities who may have difficulty getting to the polls or who live more than 20 kilometres from the polls. Others, such as Estonia, have implemented Internet voting to supplement advance polls, allowing anyone to cast a ballot from home, provided they do so a few days prior to the election.

Before voters can cast a ballot, they will need some way to confirm their identity. This can be done through biometric systems or multiple factors, such as a combination of voters' personal information with a passcode issued by the electoral authority (Goldsmith 2011). Estonia, for instance, mainly relies upon a national identify card that is swiped like a credit card on a card reader that can be hooked up to a computer.[3] The state of Gujarat, in India, sent out election personnel to manually confirm voter identity for a small fee, and voters were then given a biometric card and personal identification number (*Urban Development and Urban Housing Department Orders*, rule 6A3). New South Wales allowed voters to register over the phone or online, but they had to already have their name on the voting register. Some implementations in Norway and Switzerland involved sending voting cards to all registered households and allowing voters to log onto the system using a personal detail such as a birthday. For security, passwords were provided by a secondary method.

Most of the systems provide officials with the online results that they then combine with traditional results, although Australia requires the ballots themselves to be printed and then counted at the same time as postal ballots.

---

[2] Voting by telephone is another example of voting in an uncontrolled environment and was used in New South Wales alongside Internet voting in the last state election.

[3] Estonia's national identity card is used for a wide range of government services, including social assistance and transit.

Advantages of E-voting in an Uncontrolled Environment

Voting through the Internet presents far more advantages than using electronic methods as an alternative to paper balloting at a controlled site. It may encourage participating in the balloting process by many voters who are currently discouraged by the time and inconvenience of having to attend at a physical location. Rural voters may find the travelling distance to the polls to be a hardship; some voters may have very little time to spare given their occupational or domestic responsibilities. Some may have responsibilities to care for children, or persons with illnesses or the elderly, and not wish to leave those in their care; others may themselves be tired, ill or physically disabled, and find the journey to the polling station difficult or impossible. Internet voting may be a means of increasing overall participation rates and in some respects increasing equality of access.[4]

Risks of E-voting in an Uncontrolled Environment

Public commentary on Internet voting includes perspectives that are highly sceptical, often including assertions that the inherent technological risks simply cannot be overcome.

Proponents of Internet voting have sometimes pointed out that there is a long track record of using the Internet for sensitive transactions in the financial services area. The material interests of those involved in these transactions are high, and the incentive to fraudsters is substantial. Yet electronic systems of registering and transmitting financial transactions are routine in Canada and internationally.

Sceptics respond that there are major differences between the commercial and political contexts (Smith 2006).

With financial transactions, institutions enhance the security of transactions by insisting that users identify themselves in a reliable manner, and record and maintain the user's identity in connection to the transaction. With voting, by contrast, there is a strong emphasis on secrecy. In paper balloting, no permanent record is maintained that links an individual to a choice.

Additionally, sceptics of Internet voting might also argue that the user has a choice of whether to use technological or traditional means with financial transactions. The consequences of failure or tampering are primarily a matter for the user and financial institution to resolve, and may have little or no effect on third parties. In elections, however, a choice is being made about who will exercise government power over the entire community. The consequence of system failure could affect everyone, including individuals who wished to register their own vote only by traditional methods.

With financial services, the user also has a choice about which financial institution to use; a client can steer clear of those whose record of technological reliability or security seems dubious, or whose system seems unduly time consuming or difficult to use. The voter who is unhappy with the technological options offered by Canada's electoral system does not have the ability to switch to another provider of voting services.

The point can also be made that financial transactions take place many times a day, and the individual user is likely to engage in a number of transactions in a given year. As a result, both the institution and the user can identify problems, learn from them, and acquire considerable facility in using technologies. By contrast, federal general elections are an infrequent event in Canada – one every three to five years is typical – and there may be far less opportunity to incrementally observe both the objective features of a system and the facility of clients and institutions in operating them. With a limited window of usage for deployment and real-world testing, there may be room for vulnerabilities in the server or potential for collusion or manipulation by insiders who could attempt to modify votes by hiding program-altering code within a server (Jones and Simons 2012).

[4] There has not been a significant uptake in voting where Internet voting has been introduced; however, long-term voting statistics are not yet available, and only Estonia has used Internet voting in an unrestricted general election.

It can be further argued that the consequences of failure can be better managed in the financial services context. There may be a limited amount of malfunctioning of fraud in a large pool of transactions. When problems are detected, the user can be compensated by the institution, at least if it is not the user's own fault. The costs of compensation can be drawn from greater revenues or the cost savings achieved by operating the electronic system in general.

In the electoral context, a system failure, or perceived failure, might at least temporarily, or for a number of years, result in state authority being exercised by office holders who have not legitimately earned it, or might erode public confidence in whether authority is legitimately held. As one of the critics of Internet voting pointed out, "All an attacker has to do is to create the impression that something went very wrong. The losing candidate will do the rest" (Rubin 2007, 2). Not all of the risks involve actual manipulation or problems with the integrity of votes cast. A denial of service attack, such as happened against the New Democratic Party (NDP) in March 2012 when online voting in its leadership contest was slowed for several hours, risks disenfranchising voters if it can temporarily overwhelm the system and render it unusable for authorized voters (Geist 2012).

Proponents of Internet voting might point to case studies where it has been successfully used. A large part of this report will consist of canvassing the lessons of experience with voting in other countries or at the local level within Canada. There appear to have been some successes, including national-level voting in Estonia, and local-level voting in Norway and several locations in Canada, including Halifax and Markham, Ontario.

There is also a potential social inequality objection to Internet voting. While proponents might argue that it might reduce the difficulty of voting at a polling place for a variety of citizens (e.g. persons in geographically remote locations, those with care-giving responsibilities and persons with disabilities), it might exacerbate inequality in certain respects. The literature on the Internet speaks of the "digital divide" – a schism in society between those who have access to the online world and are adept at using it, and those who may lack access (due to affordability or location) or who may be uncomfortable with it. The ranks of such relatively disadvantaged individuals may disproportionately include members of groups that are entitled to protection from discrimination under the *Canadian Charter of Rights and Freedoms* and the *Canadian Human Rights Act*. Communities not equipped with Internet service may include remote Aboriginal communities. Those without the financial resources to access the Internet may disproportionately include individuals such as recent immigrants, the elderly or again, Aboriginal communities.

The concept of "discrimination" under the Charter and the *Canadian Human Rights Act*, it should be emphasized, is not confined to intentional adverse treatment on the part of the state. There is a duty to avoid "adverse effects" discrimination; to avoid enacting and implementing laws and measures that have the practical effect, even if unintended, of placing disproportionate burdens on bases that are prohibited by the Charter or the *Canadian Human Rights Act* (e.g. ethnicity, age, gender). Public authorities have a responsibility to accommodate, to the point of undue hardship, the needs of those who might otherwise sustain burdens on such impermissible grounds. When considering e-voting, authorities have the responsibility to ensure that when drafting a legislative framework, even if unintended, the practical effect of the framework should not be to discriminate against any voters.

Each of the challenges presented by sceptics must be taken into account in crafting a legal framework for Internet voting.

With respect to the technological objections, attention must be given to the potential for hardware malfunction or software tampering, to ensure that either can be detected in time to prevent harm before balloting is concluded, or at least that corrective measures can be taken afterwards.

With respect to the concern over loss of voter secrecy, means may be considered to lessen or overcome the risk, such as permitting a voter to use remote means to cancel and replace an earlier vote (when the voter might have felt under observation or pressure) or to vote on the regular election day and replace an earlier electronic vote with a paper-based one.

With respect to concerns over equal access to the ballot, consideration should be given to measures that will increase access to the necessary technologies, such as permitting voters to vote by relatively low-cost means such as cell phones or tablets, rather than desktop computers; to permit voters to use publicly accessible computers to vote, such as those that might be maintained at libraries or government offices; and to provide support for voters who are less familiar with technology, such as providing user-friendly means of voting along with clear and simple instructions, and access to phone help lines.

Even though one can look at technological attempts to minimize the risks associated with Internet voting, it is crucial to recognize that it is not sufficient to render the voting system intrinsically trustworthy. The system must in practice be trusted by the Canadian public, and not only by a particular group of government bureaucrats or information technology specialists who work on the project. The paper-based voting at public balloting stations has earned a large measure of trust from Canadians through long use, simplicity and transparency. If Internet voting is to secure mainstream acceptance, there should be transparency in how the system works. Pilot projects that test the system ought to be implemented, with significant effort made by electoral authorities to explain how it works; what security measures are in place; and how malfunction or tampering will be deterred, detected and remedied.

Another crucial point to recognize in designing a legal framework is that attention must be constantly given to how things can go wrong, and to institute a framework for detection, containment and remediation. It appears to be a natural human tendency to think in terms of optimistic scenarios (Kahneman 2011). However, in designing a legal framework, it is the negative scenarios that require our attention.

Threats to an electronic voting system may come from those motivated by political purposes or from technologically sophisticated individuals with no other purpose than to prove that vulnerabilities can or do exist.

E-voting in a Controlled Environment (Supervised Voting)

Mechanics of E-voting in a Controlled Environment

A controlled environment is one managed and supervised by the government. Electoral authorities provide the hardware and access to it. Voting in controlled environments uses electronic methods that are similar to those used when voting at a polling booth.

Elections officials may choose to use a custom or standard stand-alone kiosk (not connected to the Internet) that allows users to cast ballots. E-voting in a controlled environment is perhaps the most common alternative form of voting, since large countries such as India and Brazil, as well as many electoral officials in the United States, have already adopted this. The introduction of voting machines in India replaced some 2.5 million ballot boxes that needed to be secured (Kumar 2011). Voters are still required to physically attend a polling station and properly identify themselves to electoral authorities before being permitted to use a voting machine. Most of these machines are stand-alone kiosks, meaning that they are not connected to the Internet.

Advantages of E-voting in a Controlled Environment

Many Canadians are familiar with the fact that voting in the United States is often conducted via electronic voting machines. In the United States and other jurisdictions, voting machines were chosen because of the general complexity of counting voting results from various elections and referendums that were held simultaneously. Electronic machines were introduced to replace older machines using levers. In some South American countries, such as Brazil and Venezuela, the motivation behind moving to voting machines was primarily due to a lack of trust in local elections officials, and a genuine perception that voting equipment would provide more reliable results that were relatively immune to manipulation by voting authorities (Alvarez et al. 2011).

The advantage of controlled voting over uncontrolled voting is that many of the checks and balances of the current process remain, including ensuring that voting is done privately and that only eligible voters are allowed to cast the vote. Voting machines may either store the electronic votes in their memory, to be manually transferred to a central vote counting system, or may be connected to the Internet to automatically transfer the ballots to a centralized computer where they would then be counted.

Risks of E-voting in a Controlled Environment

As with other technologies for voting, voting machines must be both intrinsically trustworthy and actually trusted by the public. A potential risk is that malicious software may be installed on one or a number of the machines that may alter the results. Hardware malfunctions are also potential. For instance, Ireland had spent 50 million euros on purchasing voting equipment, but eventually scrapped it after issues arose with how the machines handled the country's more complex voting system,[5] and the decision became over-politicized (Melia and Byrne 2012). Similarly, the Netherlands banned voting machines after a report showed that it was possible to install malicious software on the specific type of system it was using and even to uncover how a voter voted by monitoring electromagnetic signals produced by the analog monitors that were used at the time (Gonggrijp 2006).

One of the major challenges of controlled e-voting is guaranteeing that the software running on each of the machines corresponds exactly to that which has been approved (Lundell 2007). As each machine may record hundreds of votes, all it may take is a small number of machines to have malicious software installed to alter an election. There has been much debate regarding whether the machines should leave a paper trail or some independent means of verifying that all votes were accurately cast and counted. The variety of available equipment on the market has led to the establishment of certification programs to ensure that the machines perform as they are supposed to, including requiring testing for accessibility and conducting physical security procedures designed to ensure the systems have not been compromised.

Controlled electronic voting may not present as many technological challenges as uncontrolled or Internet voting. Every voter uses the same kind of machine in a similar environment. A machine can be designed, inspected and its use supervised by government. However, our case studies show that the value of controlled voting tends to be outweighed in practice by its expense and risks of malfunction or tampering. There are upfront purchase or lease costs and additional costs may be incurred to securely store or move the machines between elections.

There may be advantages in controlled voting where balloting involves the voter registering many choices (such as choosing candidates for multiple offices) or potentially (as was considered in Ireland) for streamlining a time-consuming and complicated voting system. However, in Canada, federal elections continue to be based on the first-past-the-post system. A fairly small number of candidates are listed on a ballot, and the voter selects only one.

Moving to stand-alone e-voting at polling places instead of a paper-based system would likely decrease the transparency and increase the expense of an election without providing any real benefit to the average voter. There may be a limited use for stand-alone e-voting as a supplementary voting method for voters who otherwise could not vote unassisted. One such use was piloted in the by-election in the federal electoral district of Winnipeg North in 2010, to assist visual impaired and disabled voters to fill out ballots, relying on a voting machine instead of a person to assist them (Elections Canada 2011a). In such a situation, the machine could read a ballot to a voter and help them record their choice. The ballot would then be printed and counted alongside the ballots of other voters.

[5] Ireland uses a preferential system called the single transferable vote, where voters vote for multiple candidates and rank them by preference. This voting system required the voting machines to randomize how ballots were counted.

In addition to stand-alone e-voting, there may also be a desire to allow a voter to cast an Internet ballot in a controlled environment. Potential usages could include voters in the military, prisoners or overseas voters casting ballots at embassies or consulates.

The main focus of this study is Internet voting in an uncontrolled environment, and our recommendations will chiefly focus on establishing a framework for Internet voting. However, a few brief observations at the end of this report are presented for adapting these recommendations to e-voting in a controlled environment, specifically focusing on instances where a voter may cast an Internet-based vote in a controlled location.

The Right to Vote

When developing a specific legal framework for Canada, it is useful to look briefly at international legal frameworks to examine if there are any constraints or requirements regarding voting rights that must be taken into consideration. While there are general documents such as the United Nations *International Covenant on Civil and Political Rights* (ICCPR) that define some of the basic values surrounding free votes, there is no uniform set of criteria that has been released for e-voting in any convention that Canada has signed (US EAC 2011). The ICCPR specifies that citizens have the opportunity to "vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors" (*International Covenant on Civil and Political Rights*, article 25(b)).

It is important also to realize that in Canada, the Constitution of Canada, including the *Canadian Charter of Rights and Freedoms*, and not international public law, is supreme. The incorporation of international agreements into international law is properly the role of Parliament or the provinces. However, the court may construe the Charter in a manner that is compatible with international agreements to which Canada is a party.

Surveying the international treaties, including documents such as the Organization of American States's *Inter-American Democratic Charter* (OAS 2001), broad principles emerge, such as holding regular free and fair elections based on a secret ballot and universal principles. Most of the treaties, however, only cover broad principles that are found in our current system and do not specifically address issues with online voting. The only current international standard covering any form of e-voting is the Council of Europe's Recommendation Rec(2004)11 (COE 2005), discussed later, but these recommendations are not binding on Canada.

Canada's Charter has two provisions that are especially relevant to voting. One is the s. 3 requirement that "Every citizen of Canada has the right to vote in an election of members of the House of Commons or of a legislative assembly and to be qualified for membership therein." Also pertinent is the s. 15 equality guarantee, which can be used to ensure equal opportunity.

The right to vote has been described in the courts in Canada as both the right "to effective representation" (*Reference re Prov. Electoral Boundaries (Sask.)*), 160) and generally including "values embodied in a democratic state" (*Haig v. Canada*, 1031). McLachlin J, then a member of the Supreme Court of British Columbia, had listed the following included rights (*Dixon v. British Columbia (Attorney General)*)[6]:

1. The right not to be denied the franchise on the grounds of race, sex, educational qualification or other unjustifiable criteria;
2. The right to be presented with a choice of candidates or parties;
3. The right to a secret ballot;
4. The right to have one's vote counted;
5. The right to have one's vote count for the same as other valid votes cast in a district;
6. The right to sufficient information about public policies to permit an informed decision;

[6] These rights were originally described by Boyer 1981.

7. The right to be represented by a candidate with at least a plurality of votes in a district;
8. The right to vote in periodic elections; and
9. The right to cast one's vote in an electoral system which has not been "gerrymandered" – that is, deliberately engineered so as to favour one political party over another. (*Dixon v. British Columbia (Attorney General)*, 16)

McLachlin J added a tenth precept, that of the right to voting representation by population.

In the course of deciding practical cases, courts have clarified and qualified some of these general formulations of voter rights. For instance, the courts have explained that a voter's right to an informed decision requires voters to be "reasonably informed," and this requires that candidates have a "reasonable opportunity" to communicate their policies to a voter (*Figueroa v. Canada*, 914).

Thus, Canadians have a constitutional right to vote. Embedded in the right to vote is a set of values. To ensure those values are meaningful, the government may have to ensure the legal framework for conducting elections allows Canadians to take advantage of those values.

Section 3 of the Charter places a positive obligation on the state to uphold the right of participation in the voting system. This positive obligation requires that "[e]very reasonable effort should be made to enfranchise citizens" (*Haig v. Canada*, 1048) and recognizes that "[c]itizens cannot exercise s. 3 rights on their own, without the state's involvement" (*Figueroa v. Canada*, 981).

If traditional voting methods are unable to accommodate disabled voters who have a difficult time making it to the polls, remote voters or Canadians who are outside of their voting districts, then investigating or embracing proven technology could be considered a government obligation. Accommodation is important, as "the fairness of the system involves looking at how each citizen fares in relation to others" (*Figueroa v. Canada*, 981).

In *Hoogbruin v. A.G.B.C.*, the British Columbia Court of Appeal held that s. 3 of the Charter, with its affirmative duty on the part of government to take steps to facilitate voting, required the province of British Columbia to make provisions for voting by otherwise eligible voters who were outside of the province during an election.

In *Henry v. Canada (Attorney General)*, at issue was the legislative requirement that a voter produce a piece of identification, proving identity and place of residence, from a list of approved documents. The plaintiffs contended that this requirement discouraged or prevented voting by individuals from various groups, including Aboriginal voters, Aboriginal voters from rural areas, homeless voters, low-income voters, voters with disabilities, elderly voters and voters without government-issued identification bearing their names and addresses.

Justice Smith, in her ruling in *Henry*, reviewed the case law on s. 3, and concluded that it places a strong facilitative role on governments to provide opportunities to vote to all citizens and to avoid placing extra burdens on particular groups of voters:

> Section 3 rights are "participatory in nature" (*Figueroa* at para. 26) and the *Charter* creates a positive obligation on the state to put in place appropriate arrangements for the effective exercise of the right to vote… (*Henry v. Canada (Attorney General)* paragraph 140)
>
> In creating the election apparatus, Elections Canada must ensure that the process of voting is as easy and straightforward as possible for all voters. The *Charter* value of equality (set out in s. 15 of the *Charter* and recognized in a number of cases: ….) comes into play in ensuring that s. 3 of the *Charter* is understood and interpreted in a way that maintains the *Charter*'s underlying values and internal coherence. No group or category of voters should be disproportionately burdened by the requirements imposed for voting, even if the requirements are, on their face, neutral. The government would not be meeting its obligations to conduct fair elections if it failed to take steps to ensure equal access to polling stations and to accommodate Canadian citizens, in all of their diversity, in becoming registered electors and exercising their right to vote. (paragraph 143)

Essentially, Justice Smith's analysis seems to suggest that the affirmative duty under s. 3 of the Charter to facilitate voting should be construed in an egalitarian manner; that it extends to concerns to ensure that no group of voters is adversely affected; and that it is not confined to s. 15 protected groups, but can extend to other bases of inequality. For instance, while the Constitution of Canada generally does not require the government to provide the poor or homeless with economic services, the right to vote would require additional steps to ensure these people can exercise their right to vote.

While the goal should be to make it easy for every eligible Canadian to vote, the Constitution of Canada only requires the government to take steps that can be reasonably justified. Justice Smith concluded that the voter identification card requirements in the *Canada Elections Act* prima facie breached the Charter, but were "saved" by the "reasonable limits" clause in s. 1 (*Henry v. Canada (Attorney General)*, paragraph 145). The right to vote under the Charter can be justified if a restriction on voting is a proportionate means of achieving an important public interest such as ensuring that unauthorized voters do not affect the results of an election.

Parliament and Elections Canada have a duty to take reasonable measures to accommodate and facilitate voting, which may include the use of Internet voting. While it is unlikely that a court would prescribe a certain way to vote, the government is still under a duty to consider whether the current alternatives, such as postal or assisted voting, best accommodate the diverse voting needs of the electorate. For instance, blind and otherwise disabled voters may have a difficult time casting a vote in secret without some sort of assistive technology. Section 3 of the Charter also intertwines with requirements of the *Canadian Human Rights Act.* Ensuring accessibility may also be considered an inherent s. 3 requirement, as "voting is one of the most sacred rights of citizenship and that includes the right to do so in an accessible context" (*Hughes, James Peter v. Election* [sic] *Canada*, paragraph 62).

On the other hand, even if Internet voting is the best way to facilitate voting, the government may be justified in avoiding it based on concerns about cost or the integrity of the vote.

In considering Internet voting as a means of addressing the constitutional duty to facilitate access to voting, Parliament must also consider – under s. 3 as well as under s. 15 – whether doing so has the practical effect of disadvantaging certain groups of voters. There are potential tensions between the goal of generally increasing accessibility to voting and maintaining equality. Internet voting might facilitate greater participation in elections in general, but in doing so disproportionately favour those who are fairly prosperous, young and technologically adept, and those living in well-wired urban communities. It might increase the voting rate among such persons disproportionately in comparison with groups that include the poor, elderly and uneducated, and those residing in remote areas, including some Aboriginal communities.

The issue of discrimination associated with the "digital divide" and Internet voting was actually raised and tested in the United States in Arizona (*Voting Integrity Project v. Fleisher*). There, a civil rights argument was made against electronic voting in that it would be more advantageous to white voters to have an online vote and thus would dilute the voting capacity of Latinos and other racial minorities, who in 2000 had a fairly low computer usage rate. The court, however, found that since alternatives to online voting existed, such as traditional mail-in ballots, there was no violation.

An evaluation of whether Internet voting disadvantages any group would have to take into account the extent to which the existing system tends to disadvantage certain groups. Design and evaluation of Internet voting would also have to consider the extent to which the government has made a reasonable effort to address inequalities, even if it is not fully successful in doing so. Among the measures that can be considered are permitting Internet voting via tablet computers or cell phones, rather than only desktop computers; facilitating access to Internet voting at free and publicly accessible computers, such as those that might be found in public libraries; subsidizing improvements in Internet connectivity for remote areas, including First Nations reserves that currently lack it; and carrying out programs to inform and educate the general public about Internet voting, supplying user-friendly instructions and maintaining phone help lines to walk individuals through the process.

It should be noted that it would likely not be constitutionally problematic for Canada to confine Internet voting to members of groups that currently tend to be disadvantaged, such as persons with physical or mental disabilities that make on-site polling difficult or persons who live in areas remote from polling stations. Section 15(2) of the Charter has been construed by the Supreme Court of Canada as precluding s. 15 challenges to programs that have an affirmative action character. While there is no express counterpart to s. 15(2) in s. 3 of the Charter, a court would likely be sympathetic to a "reasonable limit" argument that the Government of Canada, when setting up Internet systems, is justified in focusing its attention and resources on persons who are currently disadvantaged.

One of the areas not fleshed out in Canadian jurisprudence regarding the right to vote is whether there is an inherent right to a transparent electoral process. Is there an implied duty of transparency with respect to the conduct of elections under s. 3 of the Charter? Must there be adequate opportunities for the public to scrutinize whether the voting process is properly registering and counting voter selections? This was not identified directly in the Dixon decision, although the corollary to the "right to have one's vote be counted" would logically imply a right to know that one's vote is counted.

A German Federal Constitutional Court case (*BVerfG, 2 BvC 3/07*) addressed this very issue. The court effectively banned kiosk-style voting machines because they violated the "public nature" of elections by not providing the sufficient transparency:

> The public nature of elections is a fundamental precondition for democratic political will-formation. It ensures the correctness and verifiability of the election events, and hence creates a major precondition for the well-founded trust of the citizen in the correct operation of the elections. (*BVerfG*, *2 BvC 3/07*, paragraph 107)

The German court found that a reliable correctness check would be needed, and that it was up to the legislature to ensure it existed. The voting machines in question were not examinable by the public and voting officials, and questions arose whether the results were beyond manipulation. Perhaps pertinent to Canada, the German court found that the fully public nature of elections could be tempered by other values such as achieving as comprehensive participation in the elections as possible (*BVerfG*, *2 BvC 3/07*, paragraph 128).

The requirement of transparency, at least to some extent, is likely to be a value that the courts could find inherent in s. 3 of the Charter.

Functional Equivalence to Current Voting Legislation

Courts have developed the constitutional jurisprudence by examining the contents of actual election statutes and determining what general principles underlie the details. One can look at rules and procedures to determine their functions (or objectives) in order to determine how the rules can be applied in an equivalent way under a different context. This is known as functional equivalence.

As an illustration of functional equivalence, before being allowed to vote at a polling station, a voter is required to show identification (to ensure only eligible voters can vote) and is given a blank ballot to put in a sealed ballot box (to ensure anonymity). An absentee voter must apply to the electoral authority and then will be mailed a blank ballot, an envelope for that ballot and an outer envelope that he or she is required to sign. The purpose of the outer ballot is allow the electoral authority to verify that the voter is an eligible voter, while ensuring the person opening the envelope cannot see the actual ballot (to ensure anonymity). These are different procedures aimed at equivalent functions: secrecy and ensuring only eligible voters vote.

The functional equivalence principle requires that legislators identify the purposes served by traditional means of voting, and then establish a legal framework to ensure that e-voting rules also accomplish those purposes.

The challenges in drafting legislation for Internet voting are similar to other adaptations of traditional law to allow technology. For example, the United Nations Commission on International Trade Law (UNCITRAL), in drafting model legislation for e-commerce and digital signatures, used four pillars to shape its framework: non-discrimination, functional equivalence, media and technology neutrality, and party autonomy[7] (Castellani 2010).

These principles apply to Internet voting, in that the legislation should not limit technological choices unduly or be designed so that only a certain vendor or technology may be used in cases where a better technology or solution may exist (which is the principle of non-discrimination). Functional equivalence requires that regulations affecting technology should allow it to be as good as or better than the current system, while ensuring that proposed laws reflect the purposes and functions of the traditional law (United Nations 1999). Thus, how can the purposes and functions of a normal law be made compatible with technology?

Functional equivalence is common in Canadian law relating to technology. Ontario's *Electronic Commerce Act, 2000,* lists a series of functional equivalence rules that recognizes when an electronic document can be used instead of a paper one, including the criteria for assessing reliability in light of all the circumstances and whether the information remained complete and unaltered (s. 8). It also mandates which rules do not apply and which ones can be substituted. Quebec's *An Act to Establish a Legal Framework for Information Technology* also requires the application of functional equivalency. Under this Act, technology can be used if a document meets all the legal requirements and fulfills the functions of the original system. Special attention is provided to measures ensuring integrity.

1. Integrity is ensured if it is possible to verify that information has not been altered (s. 6).
2. Integrity is preserved throughout the technology's lifetime, from creation to destruction (s. 6).
3. In assessing integrity, particular account must be made to security measures (s. 6).
4. Where information contained is confidential, confidentiality must be protected by means appropriate to the mode of transmission (s. 34).

Additionally, Quebec's Act allows additional regulations to be created by the government based on "technical norms or standards approved by a recognized body" (s. 8) and anticipates the creation of a "multidisciplinary committee" of members with information technology experience to make appropriate guidelines regarding technical standards, encryption methods and more (ss. 63, 64 and 65).

Applying these standards to the task at hand, the issue is how to ensure that the current electoral values or expectations are kept intact, while identifying specific legislative changes to be made to ensure electronic voting is as good as or better than current similar procedures. To do so, one can look at how voters vote, how their identity is checked, how various parties oversee the election results and how recounts or election challenges could occur.

There are actually four possible approaches to functional equivalence, involving various comparators.

1. Is an electronic system superior to, or as good as in all respects, in-person voting at a voting station? (This is referred to as the gold standard or "Pareto superiority.") That is, no single aspect (such as secrecy) is lessened, and at least some aspects (such as accessibility) are improved.
2. Does an electronic system, on balance, serve the core values of voting in person at a voting station? That is, the guarantee of secrecy may be lessened while another value, such as accessibility, may be improved.
3. Is an electronic system superior to, or as good as in all respects, special or mail-in voting?
4. Does an electronic system, on balance, serve the core values of special or mail-in voting?

[7] Our recommendations encompass three of these four pillars. Non-discrimination is the concept that electronic and non-electronic documents be given the same legal weight. The exception, party autonomy, is the principle in e-commerce that parties can choose the governing law, which is inapplicable in an electoral context.

Many of the principles of voting are related to the risks. For many commentators, the risks associated with online voting are analogous to postal voting used for special ballots (Alvarez and Hall 2008). Postal voting has increased risks, such as security of the ballot and uncertainty whether a ballot may ever reach its destination. Secrecy is also entirely dependent on proper procedures being followed in any remote system in separating the identity of a voter from their vote (usually by using an inner envelope with a ballot and an outer envelope with the voter's signature). An Australian court found that the provisions of mail-in balloting violated the secrecy of the vote, but the practice was allowed as an alternative means to facilitate the right to vote for those who would otherwise be unable to discharge their obligation to vote (*Yarran v. Blurton*). Likewise, there is no opportunity to verify who is actually filling out a ballot or whether a voter is being observed in casting their ballot.

Even in-person voting has risks, as evident by the extensive lists of potential voting offences that exist to mitigate abuses. Recounts often show large inconsistencies in ballots due to human error, voter impersonation can occur and a high level of discretion is often used in disqualifying ballots that appear to have any irregular marking. As Justices Moldaver and Rothstein recently stated, "[g]iven the complexity of administering a federal election, the tens of thousands of election workers involved, many of whom have no on-the-job experience, and the short time frame for hiring and training them, it is inevitable that administrative mistakes will be made" (*Opitz v. Wrzesnewskyj*, paragraph 2). In stating so, the justices set aside strict compliance with the *Canada Elections Act* in favour of finality and legitimacy of the results.

Instead of perfection, decision makers should look toward the threshold of risk or error that can be accepted. The question is, "given that no system can be 100% secure, what level of risk can be accepted for such a fundamental democratic process as voting?" (US EAC 2011, 7).

The *Canada Elections Act* clearly defines criminal acts, such as manufacturing a ballot box with a fake compartment or printing additional ballots, and uses a combination of penal deterrence, voting procedures and the appointment of scrutineers by political parties to minimize the potential for fraud or manipulations.

From reviewing the literature, it is clear that no electoral mechanism (electronic or paper) can ever be absolutely secure from every possible error or risk. The greater question is: Can the regulatory framework and associated legislation (regarding electoral offences and election oversight) provide voters as well as political stakeholders sufficient confidence that risk is minimized and that contingencies are in place to cover the range of foreseeable circumstances?

Case Studies on E-voting

Canada is not the first jurisdiction to examine Internet voting, and other places have developed their own legal framework for e-voting in an uncontrolled environment. This paper primarily analyzes legal frameworks from four jurisdictions – Estonia, New South Wales in Australia, Switzerland and Norway – but also looks at France's parliamentary elections for voters abroad and municipal tests in Ontario and Nova Scotia.

Our general observation from the four primary jurisdictions is that a high level of planning and testing were involved in advance of conducting an e-vote. While the legal frameworks in some cases were overly informal or ad hoc, the electoral authorities often adopted policies and procedures that ought to be mandatory.

Estonia

The most widespread use of e-voting has been in Estonia. In the 2011 parliamentary elections, more than 140,000 Estonians voted over the Internet, amounting to nearly a quarter of all votes (Estonian National Electoral Committee, n.d.). Estonia has allowed its voters to cast a ballot over the Internet in local elections since 2005 and national elections since 2007 as part of the government's e-government strategy (Barrat i Esteve et al. 2012b). E-voting is generally seen as secure, because voters utilize a national digital ID card that has also been used for services such as tax filing, insurance and public transportation (OSCE 2007). Additionally, Estonia has

taken steps to counter concerns about third parties putting illegal pressure on people casting a vote over the Internet, by allowing them to revote.

While e-voting has been used in five major elections in Estonia, there has been some criticism that the legal framework was underdeveloped. For instance, the conditions for invalidating voting results was not formalized in legislation and there was no independent body responsible for certifying the software. In addition, the National Electoral Committee did not have its own technical expertise (OSCE 2011). Estonia's legal framework has improved since the last election, as its Parliament approved legislative amendments in the fall of 2012 that among other things established a specialized electronic voting committee and specified the authority to stop or cancel e-voting.

New South Wales

The Australian state of New South Wales, home to Sydney and with a population almost as large as Quebec, recently introduced Internet voting. Voters who were visually impaired, disabled, would be out of state at general polling day or lived more than 20 kilometres from a polling station could register to vote over the Internet. Over 46,000 voters cast their ballots in the May 2011 general election (Brightwell 2011).

Of all the jurisdictions using Internet voting, New South Wales resembles Canada closest because it uses single member districts (for at least some seats), has an independent electoral authority, and has a format for its electoral legislation that is similar to that used in Canada. However, New South Wales differs slightly in that it uses a more complex instant runoff voting system involving preferential ballots. In order to bring in e-voting, New South Wales amended its voting legislation to add a section on e-voting, including the conditions under which it could be used and specific offences. The legislation listed major e-voting requirements and gave the state's electoral authority extensive regulatory power to create specific voting procedures (New South Wales Electoral Commission 2011).

Switzerland

Switzerland is a federal state in which 26 separate cantons each administer their own elections, and voters have the right to vote on initiatives and referendums in addition to electing their representatives in the National Council. Four cantons have adopted Internet voting, a number that is constrained by Swiss laws that limit the number of voters who can use e-voting in a general election. The most relevant of these is the canton of Geneva, with a population of 460,000, that has held nearly 20 elections or referendums in which some or all voters have been able to vote online since 2003. Switzerland requires co-operation between the federal and cantonal government to administer elections (République et Canton de Genève 2009).

Acceptance of Internet voting is also seen as higher because postal voting had already been quite common and it is treated as an alternative to remote voting (OSCE 2012a). While major e-voting requirements are listed in Switzerland's enabling legislation, it lacks a set of detailed criteria that can be used to certify a system's adherence to these requirements. The Organization for Security and Co-operation in Europe (OSCE) recommended that clear, written and testable standards on certification be developed and regularly reviewed and updated. It recommended that the legal framework include requirements for security, transparency, reliability, ease of use and secrecy of the vote (OSCE 2012a).

Norway

Norway, with a population slightly larger than that of British Columbia, has taken a highly methodical and cautious approach to introducing e-voting in the country. In 2011 municipal elections, over 27,500 voters in 10 municipalities cast a vote online in a pilot project that was unique because the government focused on making the e-voting system highly transparent. While implemented for local elections, the system was designed for an eventual national election. The Ministry of Local Government and Regional Development oversaw the development of sophisticated e-voting software, and various departments of the national government hosted

various parts of the system to prevent collusion (Norwegian Ministry of Local Government and Regional Development 2011).

Norway aimed at ensuring public acceptance for e-voting, with source code published online, confirmation of votes through cell phones, web casts of de-encryption and explicit adherence to the Council of Europe recommendations (Norwegian Ministry of Local Government and Regional Development 2006). However, because e-voting was seen as a pilot project, the legal framework is very ad hoc. In particular, the regulation lacked detailed provisions related to set-up, operation, security, testing and data disposal procedures for the system and the regulations "did not define the concrete grounds for invalidating an electronic vote" (OSCE 2012b, 4). Voters expressed a high level of trust in Internet voting, only slightly below that of paper ballots (Barrat i Esteve et al. 2012a).

Other Jurisdictions

France recently used Internet-based voting to elect 11 deputy ministers to represent citizens living abroad. As a result, this became one of the largest e-voting uses to date, with over 126,000 votes being cast online (OSCE 2012c). The office of electronic voting was created to oversee the election, and was composed of elected officials and representatives of various government offices.

While France's election appeared to be very successful, the process was not fully transparent. The tender documents were not available and there was no indication that the public was consulted during the process. Nor were the audit reports, security assessments and other documents ever released to the public (OSCE 2012c).

Not every implementation of e-voting have been successful. In some cases, e-voting was cancelled before an election or has since been discontinued. Examples of uncontrolled e-voting that critics of e-voting often point to are Washington, DC; England; and the Netherlands. Similarly, e-voting in controlled environments has experienced setbacks in Ireland, Finland and Quebec. Based on our research, the lack of a comprehensive legal framework was almost entirely responsible for problems that occurred in most of these areas. For instance, most of these jurisdictions did not conduct independent testing of the systems before they were made available to the public, which could have been part of a comprehensive legal framework.

A good example of inadequate testing is Washington, DC, where an e-voting experiment was cancelled before it was even used. In that case, a university computer science department managed to cause great embarrassment when it was able to hack a test system because simple security measures were not in place (Wolchuk et al. 2012). The problems likely would not have occurred had there been independent testing before the system was allowed to go public, proper backup procedures and divided voting tasks so that no one person could gain access to the entire system.

England successfully tested Internet voting in five municipalities in 2007 and experienced no apparent problems. However, the tests were criticized because the local electoral authorities lacked internal expertise and election observers had no ability to test the systems (Open Rights Group 2007). The United Kingdom's Electoral Commission recommended that a modern legal framework be put in place before e-voting was used in the future. This would include requiring adequate testing and more transparent procedures (Electoral Commission 2007a & b).

Most other discontinued implementations of e-voting followed a similar theme, experiencing problems that a more comprehensive legal framework and extensive independent testing could have avoided. The Netherlands used Internet voting for voters from the water board districts in 2004 and out-of-country electors in a 2006 parliamentary election (OSCE 2006). However, in 2008, legislation covering both controlled and uncontrolled e-voting was repealed after a high amount of public criticism (Barrat i Esteve et al. 2012b). Most of the criticism was not directly aimed at Internet voting, but occurred after an independent report showed that controlled e-voting machines could be physically manipulated due to weak security and that there were no procedures in place to independently verify the reliability of the machines (Gonggrijp et al. 2006).

Criticism from attempts to use controlled voting in Ireland, Finland and Quebec is also generally aimed at deficiencies in the legal framework. Ireland spent millions of euros purchasing e-voting kiosks, only to have them sit in warehouses after it was found that the software installed on them contained numerous bugs. Concern was also raised about whether the kiosks were secure and auditable (Paris 2004). A report found that the software was flawed and there were insufficient procedures in place to ensure that the voting system using voting machines was transparent and the results were verifiable (Commission on Electronic Voting 2007).

Finland's Supreme Administrative Court ordered three municipalities to redo their 2008 local elections after usability problems with their e-voting systems resulted in some voters leaving the voting terminals before their votes were submitted (KHO:2009:39). The court found that voting instructions mailed to voters were not accurate. One of the problems mentioned by some critics was that the testing of the system and the integrity of the results relied far too heavily on a few information technology professionals on staff (Electronic Frontier Finland 2009). An independent audit found the machines generally secure, but possibly susceptible to insider manipulation (Karhumäki and Meskanen 2008).

Quebec experimented from 1995 to 2005 with controlled e-voting machines, but this was discontinued on the recommendation of the Chief Electoral Officer in 2006. His main concern was there was an imprecise legislative and administrative framework that did not adequately assign roles and responsibilities or address the risks inherent in electronic voting. He also recommended adopting rigorous technical specifications and security standards, and establishing an independent authority to monitor and audit the process (Elections Quebec 2006).

Canada (Municipal)

E-voting has also been used in Canada in Markham, Ontario, and Halifax, Nova Scotia. Both of these municipalities appeared to have been successful in using e-voting, although neither appeared to face any major threats. A study following the 2006 election in Markham suggests that this was because an election in a suburban municipality in Canada is likely to "fly under the radar" of many would-be hackers (E-Mergent Management Research 2010). A high level of Internet access aided the adoption (Delvinia Interactive Inc. 2004). In both cases, the legal framework was very limited.

Major Reports on E-voting

While creating a legal framework for any new technology can be challenging, experiments, considerations and reports regarding electronic voting have gone on for almost a decade.

The most extensive considerations, in our opinion, is the progress made by the Council of Europe. Established in 1949, the council is a non-binding organization composed of government representatives from across Europe whose stated goal is to "create a common democratic and legal area throughout the whole of the continent." Distinct from the European Union, the council relies on voluntary conventions among its members to create common laws and frameworks and establish best practices. The Council of Europe has taken a leadership role in Internet voting, having worked with its member states to create extensive guidelines for legal, technical and operational requirements for e-voting implementations (COE 2005).

The United States has also attempted to create lists of best practices and sample frameworks for electronic voting that can be used by states and local election authorities. An example of this is the *Help America Vote Act of 2002*, which was set up to create guidelines following some of the controversies over inconsistent and outdated voting technology that arose during the 2000 presidential election. Of note, in the United States, the election technology, procedures and specific regulations are organized on a state-by-state level, so while centralized guidelines can exist, individual states can choose to introduce their own legislation.

In addition to the Council of Europe, many of the aspects of a legal framework can also be derived from the observation of international non-governmental organizations that oversee international election results. Included on this list is the Organization for Security and Co-operation in Europe, which has had observers in

place for recent elections in Estonia, Switzerland and Norway, and provided feedback on their elections. The International Foundation for Electoral Systems and The Carter Center also released valuable reports. More thorough descriptions of these reports are in Appendix A, International Standards and Reports.

Consolidated Checklist of Values for an E-voting Legal Framework

Our review of the constitutional jurisprudence and legislation in Canada, other literature and the legal framework of other jurisdictions has led us to a list of values and attributes that we believe the ideal legal framework for e-voting should address. The values are also meant to be reasonably technologically neutral and applicable to a paper-based system as well as both a controlled and uncontrolled e-voting system.

The following normative values should be adopted by the legal framework for electronic voting:

1. **Facilitated accessibility and reasonable accommodation.** Government should be proactive in taking steps to make voting as convenient as possible, including embracing viable alternatives such as Internet voting, unless overriding reasons prevail. Voters who face challenges should be fairly treated and resources should exist to ensure those with physical disabilities and visual impairments, as well as lower income, remote and elderly voters, can also take advantage of technology.
2. **Voter anonymity.** There should be protections at all stages of the voting process to maintain the secrecy of a voter's ballot and protect voters against undue influence affecting their right to vote freely.
3. **Fairness.** All voters should be afforded similar opportunities to participate in the electoral process, including voting relatively close to election day, having access to a simple ballot, having only a single vote counted and being able to express their electoral choice or non-choice in a meaningful way.
4. **Accurate and prompt results.** Every voter who chooses to use an alternative means should have their vote cast and recorded as intended and only eligible voters should be included in the results. Processes should be in place to audit the system to ensure that this is the case, as well as to provide voters with reasonable confidence that their ballot was properly recorded. At the same time, Canadians' expectation of a timely election should be maintained.
5. **Comprehensible and transparent processes.** It is not enough that a system be intrinsically trustworthy. The public and stakeholders should be reasonably informed of all aspects of the voting system, including important safeguards, protection and even accessing and using the system.
6. **System security and risk assessment.** Safeguards must exist at all stages to discourage, prevent and monitor dangers, including external threats, internal collusion, systematic breakdowns and disruptions.
7. **Detection of problems and remedial contingencies.** Electoral officials must have clear procedures to recognize and react to problems with a voting procedure while voting is taking place to ensure the voters are not disenfranchised. Equally, there must be legal procedures for officials to identify and rectify errors or issues in a voting system that may have affected the results.
8. **Legislative certainty and finality.** The current offences, division of roles, voting periods, recount measures and other provisions currently in legislation must be reviewed to ensure they are applicable to any changes in voting processes and continue to guarantee a prompt and final outcome to the electoral process.
9. **Effective and independent oversight.** At all stages of an election, from pre-approval, implementation, voting, through approval of the results, there must be effective oversight by individuals and entities who have the experience, capabilities (including technical skill) and public confidence to ensure laws and procedures are complied with. Testing of systems, auditing of results and effective reporting back to Parliament are all needed.
10. **Cost justification and efficiency.** Finances and resource allocation are always a consideration in securing a voting system and accommodating the needs of a diverse electorate. The costs should not be grossly

disproportionate to the real benefits in accommodating voters and promoting public confidence in the process.

While these values are all important, not all can be absolute. Any voting process may have competing values, and choices may have to be made. Secrecy and accuracy may be difficult to reconcile if there is any discrepancy between votes and results. There must be ways to separate the voter from the vote: to know that one's vote was counted, but to keep that choice secret. Convenience has been limited with strong identification rules to prevent fraud. Cost concerns may limit to what extent disadvantaged groups are accommodated. It is up to legislators as well as electoral authorities, in consultation with experts and the public, to give as much substance to these values as possible in any legal framework. As Justices Rothstein and Moldaver recently pointed out about the *Canada Elections Act*:

> The balance struck by the Act reflects the fact that our electoral system must balance several interrelated and sometimes conflicting values. Those values include certainty, accuracy, fairness, accessibility, voter anonymity, promptness, finality, legitimacy, efficiency and cost. But the central value is the *Charter*-protected right to vote. (*Opitz v. Wrzesnewskyj*, paragraph 44)

4.0 Main Findings and Recommendations

A legal framework for e-voting should incorporate the values inherent in our current voting system outlined earlier, such as integrity and secrecy, and should also balance this with practical realities associated with evolving technology and internal and external threats. Upon reviewing both the academic literature and the existing implementations at national and lower levels, it becomes evident that consideration ought to be given to not only the content of any normative rules, but also the process, style and format that election officials and legislators will use in drafting a substantive framework for e-voting. This includes in particular the following:

- the level at which elements of the framework will be defined, possibly including legislation drafted by Parliament, delegated regulations issued by the Chief Electoral Officer and policies;
- the extent to which any norms should be broad and flexible, with discretion left to administrators to deal with details in context or specifically defined up front; and
- the means by which the public, political entities and experts will access information and be involved in the formulation of rules or policies, scrutiny of the technological components and deployment of the electoral system.

With respect to issues of procedure and format, as well as the substance of potential rules and policies, this paper attempts to draw heavily on examining the approaches in other jurisdictions and the actual outcomes that ensued, both positive and negative. With e-voting, the legal framework in which technology is deployed can be just as important to its effectiveness, including bolstering public confidence, as the details of which particular technology is used (Goldsmith 2011).

Format of the Legal Framework

The legal framework for e-voting will span various legal and institutional instruments. At the highest level is the *Canada Elections Act*, legislation passed by Parliament that provides details of vote counting and registration requirements for voters, specifies electoral offences and delineates the powers of the electoral authority. Other legislation, such as privacy laws or access to information laws, may also become part of an e-voting legal framework. Additionally, the legal framework may also include instruments created by the electoral authority. For instance, government agencies may be given the power under their enabling legislation to create binding

regulations. The legal framework also includes non-binding instruments, such as policy statements and internal directives, that help define how the electoral authority plans to meet its statutory duties.

Generally, defining key issues in legislation increases democratic legitimacy by ensuring that elected representatives have a chance to debate and pass laws. The drawback is that any changes to legislation may require a significant time frame to make even minor changes. Some items, such as criminal offences, are generally only created by legislation. However, on many other issues, Parliament may delegate rule-making powers to administrative bodies. This can be done by either granting the electoral authority a broad discretion to issue regulations or by constraining its regulatory power by including specific criteria that must be met in creating regulations.

The current Act authorized Elections Canada to test e-voting, with approval of parliamentary committees, for use in a pilot project. Where other countries have conducted pilot projects, they often did so with most of the procedural requirements found in subordinate regulations and technical documents. The actual legislation was often vague, but this was because risks were low and flexibility was needed to experiment. However, OSCE reports have been critical of countries such as Estonia that have used Internet voting at a national level without sufficiently detailed legislation describing the required procedures in depth.

In a 2011 pilot project, Norway relied on technical specifications and regulations approved by the Ministry of Local Government and Regional Development, while the enabling legislation merely authorized the government to conduct tests. While Internet voting was run only at a local level, the OSCE still felt the pilot could have benefited from more formal procedures (OSCE 2012b). A report by the Ministry of Local Government and Regional Development recognized that extensive legislative amendments would be needed prior to implementing e-voting on a national basis, but found they were neither wanted nor needed for the municipal pilot (Norwegian Ministry of Local Government and Regional Development 2006).

Switzerland allows individual cantons to test e-voting, with most of the detailed requirements described in regulations issued by local cantons. The electoral legislation includes some criteria as to what the regulations must contain, such as security requirements. However, Switzerland has a very decentralized electoral system, and most electoral procedures are generally contained in local ordinances.

Currently e-voting legislation in Canada at a provincial level tends to be broadly enabling and lacks specifics. For example, Alberta's *Election Act* enables the test of alternative equipment only in a by-election with approval of the legislative standing committee, and requires the electoral authority to list which equipment will be used and what procedures need to be changed (s. 4.1(1)). Legislation regarding e-voting for municipal elections in Ontario and Nova Scotia allows municipalities to pass bylaws authorizing alternative voting methods. Nova Scotia's *Municipal Elections Act* requires the bylaws to contain measures for counting and rejecting ballots, the form of ballots and notification of voters (s. 146A). Of note, it specifically also provides municipalities the ability to create voting-related offences, with fines up to $10,000 or two years less a day in jail or both (s. 146A(7)). E-voting is only permitted as a supplementary method, requiring advance or regular voting by another means (s. 146A(6)). Ontario's *Municipal Elections Act*, on the other hand, simply permits municipalities to introduce electronic voting through a bylaw, provided the measures are consistent with the principles of the Act (s. 42).

Where Internet voting has been used in a general election, some jurisdictions have added detailed e-voting sections in their legislation. New South Wales in Australia originally authorized the Electoral Commission to conduct tests on e-voting. Before using it in the general election, however, the Legislative Assembly passed a fairly comprehensive set of amendments introducing new criminal offences, auditing requirements and key security provisions. The legislation granted the electoral authority the power to create detailed regulations following specific criteria. For example, the New South Wales *Parliamentary Electorates and Elections Act 1912* specifically authorizes the electoral authority to "approve procedures to facilitate voting by eligible electors" (s. 120AC(1)) and then provides a non-exhaustive list of criteria that should be included (s. 120AK).

Table 1 shows a brief comparison of what e-voting elements are included in the enabling legislation in various jurisdictions.

Table 1: Comparative Content of Enabling Legislation

Jurisdiction	Key E-voting Elements in Enabling Legislation
New South Wales, Australia	■ Limitations of who may use Internet voting ■ Authority for elections authorities to create procedures for Internet voting and mandatory requirements, including: – secrecy, security, authentication and printing ballots – provisions that the process must benefit those with difficulty voting ■ Audits required before and after election ■ Provisions for scrutineers ■ Specific electronic voting offences ■ Authority to create regulations overriding other acts ■ Power to terminate electronic voting ■ Mandatory reviews
Estonia	■ Specific time period for electronic voting ■ Means of authenticating/identifying voter ■ Procedures for voters changing their vote, re-voting ■ Method of counting ballots ■ Allowing use by citizens permanently living abroad ■ Provision on what happens if Internet vote is declared invalid
Switzerland	■ Authority for National Council to regulate tests, time period, availability of elections ■ Requirements regarding secrecy, prevention of abuse, counting all ballots and other measures
Norway	■ Specific authority only for municipal test projects

Table 2 lists some items covered in regulations issued by independent electoral authorities or ministries in charge of running elections. Some details of the Halifax bylaw are also listed briefly.

Table 2: Comparative Content of Subordinate Regulations

Jurisdiction	Key E-voting Elements in Regulations
New South Wales, Australia	■ In which elections Internet voting will be used ■ Voter registration and personal identification number (PIN) procedures (voters must give PIN when registering) ■ Who may use distance voting ■ Distribution of voter cards ■ Voting instructions and ballot form ■ Creation of a commission to hold cryptographic keys ■ Secure transmission and storage procedures, including tape backup of logs and failover requirements ■ Requirement of authorization and two staff to monitor any access to data requirements ■ Issuance of a receipt that will match with stored vote ■ Security provisions to ensure voter ID is not known ■ Provisions for counting votes ■ Scrutineers for printing of ballots only or later events ■ Requirement that all staff/contractors must sign steps acknowledging offences
Estonia	■ Timing of loading electoral data ■ Distribution of cryptography keys ■ Start and end time of e-voting ■ Voter identification requirements ■ Provision that paper votes cancel electronic votes ■ Quorum of National Electoral Committee required for counting votes ■ Timing for keeping electronic vote data (one month but not before final appeals)
Switzerland	■ Stipulation that approval of e-voting is limited to 10 percent of voters ■ Stipulation that approval requires secrecy, integrity of the ballots and exclusion of systematic abuses ■ Requirement for encrypted transmission of votes ■ Confirmation for voters so they know their vote is real ■ Requirement that disabled voters must be accommodated ■ Requirement that votes must be stored anonymously ■ Steps preventing data loss ■ Requirements for independent certification ■ Requirement that recounts must allow the exclusion of corrupt data

Table 2: Comparative Content of Subordinate Regulations	
Jurisdiction	**Key E-voting Elements in Regulations**
	■ Allowance of integrity tests by comparing with non-electronic votes and casting test votes
Norway	■ Stipulation that the Council of Europe recommendations are the basis of regulations ■ Permission of electronic voters to recast vote either electronically or by paper ■ Requirement that electronic voting is supplemental to traditional voting methods ■ Minimal security standards for ID, requiring voters to enter an access code sent by mail as well as a second code issued by text message ■ Requirement that information be made public ■ Stipulation that the government appoint a panel of 10 individuals with different interests to handle cryptographic keys ■ Stipulation that the e-voting system is open for one month ■ Ban on e-voting in controlled environments ■ Provisions for what happens if voter logged in when period ends ■ Requirement that all technical specifications and system code be published online
Halifax (Bylaw)	■ Specific form of ballot ■ Electoral offences ■ Stipulation that elections officials and systems elections officials are responsible for security ■ Specific provisions in requests for proposals

Achieving a balance between legislation and delegated regulations is important. The more detailed legislation in place, the greater legitimacy the legal framework will probably have. However, it is also very important whenever a government attempts to create legislation involving technology that the principles of functional neutrality such as technological neutrality be preserved and that the legislation avoids being overly detailed in some of its technical specifications, such as prescribing the precise hardware or encryption program to be used. Too much detail may "inhibit innovation or create legal 'technology locks'" (Alvarez and Hall 2008, 184). This may be of particular relevance in countries like Canada, where it may take months for simple changes to elections legislation to be approved by both houses of Parliament. As such, while the legal framework should be very extensive, many of the technical procedures are better left to regulations.

Detailed legislation is not necessarily needed to test an electronic voting system in a by-election or comparably limited context, but using it in a general election without amendments to the *Canada Elections Act* may raise public concerns about whether there has been sufficient democratic debate and support for the system, and whether sufficient measures have been in place to reduce risk, identify malfunctions or tampering and provide for remedial measures.

The *Canada Elections Act* does not clearly define issues such as how the system would adapt to the discovery of problems with the e-voting system and what corrective measures would be taken. For instance, if a serious problem were discovered with an e-voting system during an election, would the vote be discontinued? Under

what circumstances would an entire constituency result be invalidated and the election repeated? Currently, the Chief Electoral Officer has the authority to issue ad hoc adaptations to the Act in case of unforeseen challenges, but ideally the Act should be tailored to provide some general direction, and if possible, some guidance on how to resolve issues that could affect the results of an election.

Another concern is that some of the decisions involving e-voting require a balancing of values inherently present in s. 3 of the Charter. As such, any restriction on voting rights should be prescribed by law.

A parallel can be drawn to the 2009 German Federal Constitutional Court decision (*BVerfG, 2 BvC 3/07*) that blocked the use of e-voting machines until either better transparency measures were implemented or legislation specifically authorized the reduced transparency in return for greater accessibility. In that case, the Federal Ministry of the Interior was given the authority to create ordinances related to the approval of the machines. The court found that because of ongoing (and often rapid) technical development, detailed regulations are generally best left to the electoral authority. However:

> Because of their particularities, regulations relating to the deployment of voting machines are reserved for parliamentary decision insofar as they relate to the major requirements for the deployment of such devices. This includes the decisions on the permissibility of the deployment of voting machines and the fundamental prerequisites for their deployment. (*BVerfG, 2 BvC 3/07*, paragraph 136)

Many of the problems that occur when introducing voting technologies are not due to problems with the technology, but rather with a lack of ancillary process that mandate how election administrators implement the systems or interact with the technology (Alvarez and Hall 2008). Whether the issue is the hardware, software or the machine–human interface, it is the responsibility of Parliament to provide intelligible standards, minimum requirements and general directions to agencies such as Elections Canada to assist them in exercising their discretion and creating regulations or policy. This helps ensure public confidence in the use of technology and provides a stable basis to evaluate the regulations and to hold officials to account.

Access and Eligibility

Determining how and when e-voting will be used is an important step, as well as deciding who gets access to the system. Should legislators treat it as a special voting system designed purely as a way to enfranchise disadvantaged groups who may have difficulty voting, or should it be used an alternative to voting in person as a means to increase voter turnout and enhance convenience for everyone?

Currently, the *Canada Elections Act* provides three main methods of voting: voting on polling day, at advanced polls and by special ballots (s. 127). Special ballots can either be completed in person at an office of the returning officer or by requesting a ballot be sent by mail and returned. For those with physical disabilities, there is even the provision for a designated election official to go to a person's home and assist the individual in marking the ballot (s. 243.(1)).

If decision makers choose to allow e-voting, then a provision should be added to the list of voting opportunities in s. 127 of the *Canada Elections Act* along with any dedicated provisions.

Restricting Eligible Voters

One of the considerations behind e-voting software is whether to allow its use by everyone or a selected subset of voters. Is e-voting being used as a tool only to accommodate those who may have difficulty voting at a polling station? Will there be a decision to limit who can vote remotely in order to work out concerns over voter authentication and mitigate against abuse? The *Canada Elections Act* contains specific provisions to set up military polling stations (part II, division 2), as well as to accommodate disabled voters by sending elections officials to their house to facilitate voting (s. 243.(1)). The Act also differentiates between those voting by special ballot who are residing in Canada (part II, division 4) and those who are living outside the country (part II,

division 3). However, there are no restrictions on who may use special voting, as long as they meet the residential and identification requirements. Any eligible voter who does not desire to vote on voting day can either vote in advance at the office of the returning officer or request a ballot by mail.

Internationally, there are different approaches to eligibility for e-voting. In Estonia, every voter who chooses to use the system may vote online, although this process was facilitated through a national ID infrastructure already used for government services with a secure ID card, so that there was less of an issue with handling identification and authentication of voters. Switzerland's federal ordinance on political rights allows e-voting, but limits its use to 10 percent of voters at the federal level in any given election. This effectively ensures a national government can be formed, even in the event of an e-voting failure. France recently allowed only those living abroad to cast a ballot in their Parliament, thereby reducing voters' dependence on mail to return ballots; domestic voters were still required to vote using traditional means.

New South Wales recently allowed specified classes of voters to cast a ballot over the Internet. Under s. 120AB of the *Parliamentary Electorates and Elections Act*, the following categories of voters are permitted to vote over the Internet:

- electors with visual impairments
- electors with disabilities that make it difficult to reach polling stations
- rural voters who live over 20 kilometres from a polling station
- voters who will be out of the state on voting day

Additionally, the legislation grants New South Wales's Electoral Commission the ability to publish additional regulations that further restrict or expand eligibility requirements. In order to be eligible, the voters must be registered to vote in advance by applying online or by phone. The original intention was to permit only disabled voters to use the new system, to satisfy international obligations under the United Nations *Convention on the Rights of Persons with Disabilities* (Allen Consulting Group 2011). However, rural voters and out-of-state voters were subsequently authorized by the Legislative Assembly to vote over the Internet. As Australia uses compulsory voting, this ensures that mandatory participation in an electoral system does not create undue hardship.

In Canada, the Charter guarantees of an effective right to vote to all Canadians and a general presumption of equality create the possibility that the courts could find a constitutional violation if some voters were allowed to use e-voting in an election while other voters were not. Generally any restriction of a Charter right must be defined by law or regulation, in accordance with s. 1, rather than left to the unconstrained discretion of officials.[8] However, if a program is only aimed at ameliorating a disability, the Charter will not preclude it.

To avoid potential constitutional challenges, legislators would be prudent to include provisions in the *Canada Elections Act* if they wished to limit who could e-vote in a given election.

If the goal of choosing a limited deployment for online voting is to limit exposure to fraud, a better solution may be to use more stringent identification requirements, such as requiring in-person registration for most voters. This may be less convenient for some voters, but convenience (as opposed to disability accommodation) is not a constitutional requirement (*Henry v. Canada*).

Cost Effectiveness

Cost effectiveness might weigh into a judicial evaluation of whether the Government of Canada has fulfilled some of its prima facie constitutional duties (e.g. facilitating voting) or a "reasonable limits" analysis of whether an e-voting system has features that are problematic constitutionally – such as excluding or not accommodating

[8] See, for example, *Re Ontario Film and Video Appreciation Society,* (1984) 45 OR (2d) 80, discussed in Hogg 2007, 123.

certain groups of voters – but is nonetheless justified as a "reasonable limit" on a Charter right. Leaving aside the potential for court challenges, cost–benefit considerations can be decisive in public support for an e-voting system. For example, a decision to introduce Internet voting to overseas military voters in Australia in 2004 ended up costing around AUS$521 a voter compared with $10 using traditional voting means (Australian Electoral Commission 2008). A pilot project involving assisted voting devices in the Winnipeg North federal by-election in 2010 cost nearly $30,000 per vote, with only five voters using the equipment (Elections Canada 2011a).

Table 3 shows the breakdown of New South Wales costs per vote using the actual costs, as well as projected future costs if every voter was permitted to vote online (Allen Consulting Group 2011).

Table 3: Actual and Projected Costs of Voting in Selected New South Wales Elections

Use	Cost per Vote (AUS$)
46,000 votes cast electronically in 2011 state general election (disabled, rural, absentee)	$72 (actual)
500,000 e-voters in local government elections	$10 (estimated)
1,000,000 e-voters in local government elections	$6 (estimated)
Regular election	$8 (actual)

While the cost per vote to run an online system appears to be high, this must be put into context. New South Wales spent AUS$3.4 million on its e-voting system in 2011 (about CAN$3.6 million). To put this in perspective, the total cost of running the 2011 general election in Canada was $279 million (Elections Canada 2011b). The more people who can e-vote during an election, the more cost effective the system will appear.

Handling Identification

Voter fraud has been a legislative concern in Canada, and any use of e-voting or expanding alternative means of voting will likely raise this issue. Parliament passed more stringent voter identification requirements in 2007 to address concerns with voter impersonation at the polling box. Voters must now bring proper identification to vote or have another voter vouch for them.

Those voting by mail through a special ballot must provide satisfactory proof of identity but there is very little means to prove that an individual returning a mail-in ballot was the person who applied to receive it. The trade-off with special balloting is that election officials are provided with time to approve each applicant and have time to check addresses and identify multiple voters, whereas poll workers on election day are expected to instantly register a voter. If functional equivalence to mail-in voting is the only criterion applied, then an address and other identifying information should be sufficient.

Internet voting can be more secure than mail-in voting in some aspects, since personal identification information is not only collected when a voter requests a ballot, but an e-voting system could again require additional information prior to a voter casting their ballot. However, decision makers may also be concerned that introduction of a new technology may come with increased scrutiny as to the existing special voting identification requirements, and thus may want to be proactive.

Estonia may be the gold standard for identification and authentication because of its use of a national electronic identification card. The identity cards are ubiquitous across the country and used for everything from bus passes to government services. Voters insert the card, which contains a code that securely encrypts their identification, into a card reader attached to their computer while entering their secret passcode. If a voter loses their card, they can go to a bank or government kiosk to get a new card and passcode. Because a voter must prove their identity in person before gaining the card and the passcode, there is very little concern about an ineligible

individual being able to vote. While an eligible voter could provide their card and passcode to a third party, there is little opportunity for wide-scale fraud.

Other means of handling voter identification vary. In Norway, the pilot relied on both mobile phone infrastructure as well as secondary voter cards. A voter would receive a login identity and passcode in the mail, and upon logging in would receive a text message to their phone, reducing risks from stolen mail. Switzerland, on the other hand, mailed voter cards with passcodes and relied upon secondary personal information such as date of birth to reduce the potential for systematic fraud. In India, in order to vote online, an electoral officer will come to a voter's house and take biometric information from the voter, including a thumbprint, before issuing a voting card and online PIN (Kapoor 2011).

New South Wales, as mentioned earlier, imposed limitations on who may vote. To reduce impersonation or mail fraud, a voter would be provided a passcode over the phone or online when they applied to vote. Anyone making a misleading statement on an application may receive up to two years imprisonment or a stiff fine. The Electoral Commission is required to publish regulations on how authentication is handled, and the requirements may change in the future.

Many of these methods arguably provide an equal or higher level of protection against unauthorized voting or mail theft than traditional mail-in ballots that are vulnerable to mail theft. Additionally, Estonia's use of a secure identification card ensures a similar level of security as in-person voting since visual identification is required to gain the passcode in the first place. However, any discussion about whether to introduce a national identity card in Canada is beyond the scope of this paper.

While adequate steps should be taken to ensure that those using an online voting system are in fact entitled to vote, the Supreme Court of Canada has found that overly onerous steps and perfection are not a requirement.

> The system strives to achieve accessibility for all voters, making special provision for those without identification to vote by vouching. Election officials are unable to determine with absolute accuracy who is entitled to vote. Poll clerks do not take fingerprints to establish identity. A voter can establish Canadian citizenship verbally, by oath. The goal of accessibility can only be achieved if we are prepared to accept some degree of uncertainty that all who voted were entitled to do so. (*Opitz v. Wrzesnewskyj*, paragraph 45)

Because online authentication technology is constantly improving, the electoral authority should be required to create regulations describing authentication and identification procedures. In order to ensure that non-eligible voters cannot vote, the procedures should either require voters to personally identify themselves to an authorized official before receiving login information or require a sufficient combination of the voter's personal information and login pass code.

Additionally, the electoral authority may use a secure electronic signature as part of the voter identification process or in returning digital ballots. An example of legislation describing this can be found in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), as well as the *Secure Electronic Signature Regulations*. Under PIPEDA, the Treasury Board must be confident that a secure electronic signature is secure and reliable and meets the following conditions (s. 48.(2)):

> (*a*) the electronic signature resulting from the use by a person of the technology or process is unique to the person;
>
> (*b*) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;
>
> (*c*) the technology or process can be used to identify the person using the technology or process; and

(*d*) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.

Parliament should grant the electoral authority flexibility in choosing the methods of authenticating voters as long as they are secure and reliable.

Considerations for Voters Abroad

In the last Canadian election, eligible electors living outside of Canada cast over 17,000 votes. One of the benefits of Internet voting is that it makes it easier for voters living abroad to ensure their ballot arrives in time, especially since international mail can be slow. However, there may be legitimate reasons for allowing the electoral authority to limit online voting to certain countries. For instance, some countries may censor or monitor Internet transmissions, other countries may pose security concerns and it is generally difficult to punish those who violate election laws abroad.[9]

Most Canadians casting ballots abroad live in countries with a comparable level of Internet freedom as Canada. More than 11,000 of these votes came from countries that are listed as having a high degree of Internet freedom by the NGO Freedom House, including the United States, United Kingdom, Australia and Germany (Kelly and Cook 2011). An additional 3,000 votes came from other countries in the European Union that were not ranked, but likely have similar access to the Internet. There were also approximately 650 votes from states that have only partial Internet freedom, including Mexico, India, Korea, Turkey and Russia, and an additional 1,200 votes from Singapore and Persian Gulf countries that were not covered by the Freedom House listing. Some countries receive a poor rating on Internet freedom, engaging in censorship and often blocking Internet connections. Last federal election, 660 votes were cast by mail from such countries, including China, Thailand, Vietnam, Saudi Arabia, Iran, Pakistan and Nigeria. Whether there is potential for state interference in an election system in these countries may raise a concern, albeit arguably the same concerns could exist for mail-in ballots.

Another consideration is that allowing the Internet voting system to be accessed from countries that are associated with large incidents of cyber-attacks could cause security concerns. For example, a 2007 cyber-attack believed to have originated in Russia caused significant disruption to Estonia's banks and parliamentary communication for almost three weeks (Ruus 2008).[10] According to security experts, the four largest sources of online attacks in the first quarter of 2012 came from China (30.6 percent), the United States (19.2 percent), Russia (13.4 percent) and India (9.5 percent) (Prolexic 2012). Election authorities may have to block some international access in the case of a massive cyber-attack coming from a foreign country.

As well, not every country permits encrypted Internet signals to be sent abroad. Switzerland focused its online voting toward voters living in countries that signed the Wassenaar Arrangement, which is a treaty adopted by Canada that permits the exchange of encrypted data between countries (COE 2010).

We recommend the electoral authority work with other government departments to identify countries where Canadians may freely vote abroad as well as countries that may host potential threats to the voting systems. The legal framework should permit the electoral authority to determine from which countries online voting may be available as well provide them the authority to block voting from a given country to prevent attacks. Additionally, in countries where a free Internet does not exist, legislation should allow electoral authorities to set up electronic voting stations at consulates and embassies. However, additional precautions should be taken with any shared voting terminal similar to what would be required with a controlled voting system.

---

[9] Extradition treaties and international agreements on cyber security may allow some enforcement.

[10] This attack happened outside of an election period and appeared to originate from private groups unhappy with the relocation of a Soviet-era monument.

Voting Period

The legal framework, either directly in the legislation or in published regulations, should clearly define all important dates in an election period. While it is possible to allow Internet voting until the close of the polls on the final day of voting, this does not appear to be the norm in jurisdictions that allow e-voting. The Council of Europe only recommends that Internet voting not proceed past the regular election cutoff (COE 2005). However, a Norwegian report firmly recommends precluding e-voting on election day (Norwegian Ministry of Local Government and Regional Development 2006).

In most cases, Internet voting starts about midway through a campaign and ends four to seven days before the polls close. E-voting happens early to allow electoral authorities time to react to technical problems as well as revise voter lists so that election day poll clerks know who has already voted. However, Internet voting should not end too far in advance of the election day as to unfairly deprive voters of key election milestones, including debates and last-minute announcements.

In many ways this is similar to advance voting, which happens on days 10, 9 and 7 of an election in Canada. Estonia's Internet voting period ends at the same time as the advance polls; that is, four days before election day, mainly so officials can reconcile multiple votes, because the legislation permits individuals to override their Internet vote with a second Internet ballot or by voting in person at an electoral station. Estonia's online voting period starts 10 days before the election and prior to advanced voting.

New South Wales allows voters to vote online from the 12th day before an election up until the evening before the election. Voters who apply to vote online are precluded from voting at the polls. These dates are published in electoral regulations. Electoral authorities may extend e-voting up until the close of polls on election day, in the case of any major technical problems on the final day of e-voting. However, any extension of the voting period would likely cause a delay in tabulating the final voting results since the state's procedures require each e-vote to be printed and counted alongside regular ballots.

The online voting period should extend for a multiple-day period, to maximize usage as well as to prevent disruptions from affecting voter confidence. Norway allowed e-voting for one month, which was seen as an effective tool to minimize disruption from a potential denial of service attack (OSCE 2012b). If too short a voting window is permitted, the possibility of a temporary attack on a server may frustrate and potentially disenfranchise voters. This happened in Canada during the 2012 NDP leadership contest, when officials had to extend e-voting periods as a result of a denial of service attack (Scytl Canada 2012).

We recommend that the electoral authority be given the authority to define the voting period for e-voting in regulations. The voting period should begin well in advance of voting day, be accessible for a week to 10 days, and end a few days prior to election day. This would provide e-voting administrators time to revise electoral lists as well as time to react to potential problems with the e-voting system.

Summary of Recommendations

E-voting can be introduced to facilitate accessibility and provide reasonable accommodation to voters who have difficulty attending traditional voting or could be expanded to allow all voters to use the system. These decisions may involve accommodating cost effectiveness, efficiency, voter fairness and even risk assessment. As discussed in the background section, the legislative framework should treat e-voting as the functional equivalent of special ballots conducted by mail, and non-electronic alternatives should always be accessible. While electronic ballots may be analogous to paper, the constitutionally guaranteed effective right to vote likely demands that voters who do not trust or feel comfortable using computing technology are provided with sufficient options and feel confidence that their vote is secure. We recommend:

1. E-voting should be treated as the functional equivalent to special or postal ballots and non-electronic alternatives should always be accessible.

2. If there is a desire to limit electronic voting to a specified group, the *Canada Elections Act* should clearly prescribe the eligibility requirements. (Some jurisdictions only allow out-of-district voters, disabled voters and those who live a fixed distance away from the polls to vote over the Internet.)
3. Access to electronic voting should be broad enough to ensure that implementation costs are not overly disproportionate to traditional voting.
4. Parliament should grant the electoral authority flexibility in choosing the methods of authenticating voters as long as the methods are secure and reliable.
5. Electoral officials should work with diplomatic officials to determine which countries are safe to allow remote voting in.
6. The period for e-voting should be conducted over at least a week and end no earlier than the close of advance polls but before voting day. The period should be fair to e-voters but also allow the electoral authority time to react to technical problems.

Transparency

One of the major issues for building public confidence in an electoral system will be the transparency of a technological system. Transparency is important both for ensuring integrity in the underlying measures as well as building public confidence. As noted in one paper, "It is not only important that a system is reliable, it is also important that people *believe* that the system is reliable" (Pieters and Becker 2005, 3). Pieters and Becker argue that transparency may be a more important democratic value than voter secrecy, in an argument about whether a voter should receive proof of how they voted. In moving to an online voting system, transparency is directly related to the amount of information that is available to the public, as well as to intermediaries such as candidates, political parties, the media and elections observers. As was stated in a recent paper on trust in the system, "[t]he more information is withheld, the less the public will appreciate the added value gained by applying the remaining measures" (Volkamer et al. 2011, 2).

Scrutineers and Monitoring

Electoral transparency is provided for in a number of ways under the *Canada Elections Act*. The Act provides that most election instructions, correspondences and rulings are public records and may be inspected by any person during business hours (s. 541). Election officials are required to create reports if they believe that any ballots have disappeared (s. 314). The Chief Electoral Officer is also required within 90 days after an election to issue a formal report on election results and other issues (s. 534).

Political candidates or their representatives (also known as scrutineers) are an important means by which transparency is guaranteed. They are permitted access to polling stations and may be present at the counting of the votes and are able to object to the ballots as they are counted. The election rules even stipulate that if no candidate representatives are present for the counting of the votes, then two electors must observe the counting (s. 283(1)).

The current system guarantees transparency by a combination of scrutineers and reports to the public. A similar level of transparency with e-voting can likely be achieved by detailed reporting and allowing scrutineers access to components of the e-voting system. The rights of candidates, parties, citizens groups and the media to scrutinize the accuracy and efficacy of technical processes are critical to the conduct of genuine elections (Young 2009).

Use of candidate-appointed scrutineers to oversee e-voting has already been given some traction in other jurisdictions. In France's 2012 parliamentary elections, candidates were permitted to appoint a delegate to monitor electronic voting if advance notice was given (*Electoral Code*, article R176-3-2).

As well, the processes used in paper-based systems are inherently less complicated and observation is simpler, whereas specialized training may be required to sufficiently perform the role of a scrutineer in e-voting. Norway had a very open process to allow observation, but at the same time, parties showed little interest in remaining involved (OSCE 2012b).

It is important to determine what level of access scrutineers (or other observers, such as academics and international observers) have to view or monitor servers and equipment on which a voting system is run during an election cycle. Some observers feel that scheduled observations, as opposed to random checks of equipment, are "against the spirit and purpose of trustworthy election observing" (Open Rights Group 2007, 13).

Unlike traditional voting, scrutineers do not need to oversee the counting of every single e-vote; rather, they must ensure that the electronic processes are followed. The legal framework should include formal rules to ensure parties can appoint technically knowledgeable scrutineers to observe the electronic voting system.

Access to Source Code and Logs

An important legislative requirement in an e-voting system is that there are provisions to ensure that every aspect of the chosen system can be viewed and observed for either errors or manipulations. It may be sufficient for a school board election or low-risk vote to trust a vendor's system or rely on other jurisdictions' experiences with a service provider. However, it would be highly unreasonable for election officials to use a controlled e-voting system for a national election that could not be independently verified to ensure every vote is counted and that there is no opportunity for third-party manipulation. In Germany, a lack of transparent access to e-voting machines' source code led its Federal Constitutional Court to ban e-voting machines (*BVerfG, 2 BvC 3/07*).

In an Internet voting system, public transparency is needed in the selection of the hardware and platform that a system is run on, in the review of the code behind all of the e-voting software and in access to any logs or records of any changes that are made to the software.

The legal framework should address who has access to the source code and logs, describe any conditions for gaining access and outline how errors should be reported. Optimally, access to source code should be as open and transparent as possible, while protecting any proprietary or critical intellectual property (Alvarez and Hall 2008).

While the *Access to Information Act* generally provides the public with access to government documents, a more tailored regulation for e-voting is needed since the Act allows the government to withhold information about computer systems and their security measures, technical information or third-party trade secrets (ss. 16.(2), 18.(*a*) and 20.(1), respectively).

One of the options to increase transparency is to make the entire source code publicly available. Election authorities would make the code available on a public site for scrutiny prior to the start of voting. Arguments in favour of publicly available source code include: (Smith 2006)

1. Visibility of source code works as a motivator to write clean code.
2. Free analysis can be gained by making it readable to the world.
3. The available resource base for future development is broadened.
4. The counting process is open for all to inspect.

Public availability of the code was one of the measures used in Norway to increase transparency. The source code of its election system was posted on the government's website, although there are patent and copyright protections for the intellectual property rights of the software developers. Other transparency measures include a live videotaped ceremony open to the public where election administrators ran various steps in de-encrypting and tabulating the votes.

While releasing source code publicly may seem to be more transparent, the advantages of this approach over selectively submitting the code for private review may be limited. The average member of the public would not be able to properly vet the code, and there is little guarantee that undetected vulnerabilities would be reported to election authorities rather than exploited by those viewing the code.

Generally the goal is to ensure that e-voting is not overly less transparent than paper-based voting, because the principle of functional equivalence generally ensures the rules should be as good or better than the current rules. However, even under a paper-based voting system, the public relies on intermediaries to ensure the results are accurate, and access to vote counting is generally restricted to election officials and scrutineers.

While Norway allowed its source code to be made public, most jurisdictions restrict access. Estonia, for example, does not publish its code, but rather has it reviewed by an academic prior to being used, and an independent auditor is appointed to observe that technical staff have followed prescribed security procedures. Third parties can review the election software after signing a confidentiality agreement. If problems are found, reviewers must notify the election authorities before they are allowed to make public comments (Martens 2012). Likewise, the law in Switzerland contemplates and allows interested academics to review the electronic voting software, while mandating that an independent certification agency actually review the code.

While most jurisdictions rely on a non-disclosure agreement to protect the code, the state of New South Wales has taken a stricter approach, prescribing a punishment of up to six months in jail for disclosure of the source code.

Allowing qualified individuals full access to the source code is generally seen as a way to promote technical improvements, while limiting some of the potential risks with full public disclosure (Hall 2006). In the Australian state of Victoria, the Victorian Electoral Commission, currently working to implement Internet voting, has recommended the legislature create independent observer roles to provide scrutiny of e-voting systems (Buckland and Wen 2012).

Because the Canadian electoral system already provides candidate or party representatives with a high level of access to counting, it would be prudent to create a similar scrutineer role to review the Internet voting system. Even if the electoral authorities appoint an independent auditor to review the code, allowing political entities to nominate their own reviewer will increase trust. Additional access to code may be given to academics, international observers, representatives of NGOs or even members of the general public.

The legal framework should give the electoral authority the power to create a series of formal requirements on how access to the code and system information will be granted and whether there are any conditions that should restrict access. There may be requirements that individuals apply so that background checks (e.g. criminal record) can be carried out, and individuals might be required to sign limited confidentiality agreements. Also, as discussed in section 4.6.6 of this paper, an accompanying electoral offence preventing unauthorized access to the code may also be considered.

Public Communication and Compliance

Whether or not the entire e-voting source code is published, every effort should be taken to communicate as much information as possible. Source code availability does not address comprehension, although its availability may increase the level by which the public trusts the systems (Hall 2006). The specific requirements could be mandated by the legislation or may be left up to electoral authorities to determine what the adequate information should be.

In Switzerland, article 27*d*(3) of the federal ordinance on political rights stipulates that cantons must have a plan to inform the electorate about the organization, technology and procedures for the electronic voting before using e-voting.

Thorough documentation ought to be made available, as without it the public may not appreciate the system (Volkamer et al. 2011). However, simple documentation should also be released that will be understandable by the general population. This should include the technical measures taken to guarantee secrecy and ensure the integrity of the system. The benefit of this is that independent technical experts can review the system and confirm to the public that the simplified documents are correct. The perception of credibility is as important for electoral processes as actual integrity (Volkamer et al. 2011).

It may also be useful for governments to show compliance or at least assess the given system against international methods. The Council of Europe recommendations, for instance, provide detailed technical steps, which Norway specifically references in its regulations. The legislation may also choose to require the system to be compliant with a recognized body for security or data integrity. Section 68 of Quebec's *An Act to Establish a Legal Framework for Information Technology* provides an example of legislation that requires approval by a recognized body, listing the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO) or the International Telecommunication Union (ITU) and Standards Council of Canada (or a body accredited by that council) among the known authorities. Likewise, the Council of Europe recommendations list the European co-operation for Accreditation (EA), the International Laboratory Accreditation Cooperation (ILAC) and the International Accreditation Forum (IAF).

The legal framework should allow considerable flexibility to the electoral authority to develop a plan to communicate to the public the steps taken to ensure the integrity of the system, as well as any third parties that have verified the software. It would be useful, however, to formally acknowledge the importance of reasonably extensive and timely public communications and identify any particular concerns (protecting systems from tampering, the intellectual property of technology providers or individual privacy) that might limit the time and extent of public disclosure.

Reporting and Responding to Incidents

Because e-voting can be vulnerable to both external threats as well as technical problems, it is possible that problems with the system could be uncovered at any time before, during and after an election. The legal framework should address not only how problems are reported, but may also consider making it mandatory for individuals reviewing or designing the system to report any disruptions or errors to stakeholders as soon as possible.

In order to increase public confidence, some critics of e-voting contend that it should be mandatory to report defects or errors as soon as they become known (Jones and Simons 2012). This would require a positive obligation on electoral officials, candidate representatives and third parties to disclose vulnerabilities discovered while testing. For instance, in response to concerns about manufacturers of voting machines not being forthright about system errors, California enacted legislation approving a fine of US$1,000 per day for any manufacturer that uncovers an error, defect or fault in their system and fails to report it within 30 days (*California Elections Code*, s. 19214.5).

In addition, a formalized process should be implemented so that reports of electoral incidents are quickly reported to all stakeholders. While the *GC Information Technology Incident Management Plan* contains some requirements for reporting IT security incidents to the Government of Canada's newly created Cyber Response Unit, there is no public reporting requirement (Government of Canada 2012).

Once vulnerabilities are reported, a plan will need to be in place to respond to and rectify problems. Some of the potential incidents may require late patches to the systems, even after the system has been independently tested and approved. Responding to the measures may require quick fixes if they become evident during actual voting. However, any change or alteration to the system may raise questions about system integrity and the potential for manipulation of the electoral system. A clear process should be in place to handle software changes. At the very minimum, any changes should require at least two individuals present when the changes

are made, be clearly logged and communicated to scrutineers, and be available as a report to the public after the election.

Table 4 is a non-exhaustive list of some issues that have surfaced in the literature.

Table 4: Required Responses to E-voting Incidents

Potential Incident	Response Required
Problems with software client installed on home computer	Re-release updated voting software.
Malware spread with ability to affect votes	Re-release updated voting software and alert voters to run anti-virus software before voting. Potential to allow re-voting could alleviate concerns.
System vulnerability or threat intrusions	Central server update may be needed, which may pose a serious threat to the electoral process. Assessment of integrity of existing votes should be required.
Denial of service attack (attempt to overload servers with false traffic)	Server response may be needed. Voting period may need to be extended. In some cases, outside traffic (international voters) may need to be redirected or blocked.
Erroneous ballots being submitted	Will have to identify whether this is a system error or an attempt to spoil ballots.

We recognize that often suppliers may have a vested interest in not reporting problems with software. In the case of electoral software, the consequence could be disastrous. Legislation should be created to require that any known errors be reported immediately to appropriate authorities. Additionally, the electoral authority should create regulations and policies outlining how it will respond to problems and clear procedures on how updates to the software can be made.

Summary of Recommendations

Public confidence in an e-voting system will depend on comprehension and transparency. The legal framework should ensure the public has access to information about the system's integrity and security, and methods should be in place to allow key stakeholders to independently verify the security and integrity of the system.

While the implementation of electronic voting in some jurisdictions has required all e-voting source code to be published online or to use only open source code, we recognize there may be valid reasons for allowing suppliers to protect trade secrets and giving the electoral authority the flexibility to choose the most secure and reliable technology. Current legislation allows candidates' representatives to monitor all critical steps of voting. Similar steps should be taken with e-voting to ensure transparency. We recommend:

1. Party- or candidate-appointed scrutineers should be able to view all source code and inspect physical technology.
2. A formalized process should be created for academics and international observers to get similar access to ensure the integrity of the e-voting system.
3. Decisions on whether to publicly post source code or use open source technology should not be legislated, but should be left up to electoral officials.

4. Electoral officials should be required to provide public reports on the security and integrity of the e-voting system, as well as which external reviewers approve the system.
5. Legislation or regulations should ensure that observers or developers immediately report errors to election authorities.
6. Procedures should be in place to have election officials inform key stakeholders, including political parties, of security incidents.

Division of Roles and Responsibilities in Administering E-voting

A voting system is seen as trusted if it attracts voters and leads to confidence regarding the integrity of the published result and the secrecy of the vote (Volkamer et al. 2011). In a traditional election, Canadians are used to an independent electoral authority that administers an election, a comprehensive set of written elections procedures, the ability for parties to present scrutineers at important opportunities such as voter registration and counting, and the circumstances for a judicial recount. Voters may not witness their vote being counted, but they have confidence in the system based on participation of individuals whom they may trust and who operate locally.

Internet voting, while handling a function similar to special balloting, requires more specialized expertise (in information technology) than traditional procedures (Norwegian Ministry of Local Government and Regional Development 2006). There is also a need for a greater division of roles, as the system is far more centralized and there is a greater risk that the election results or voter privacy could be compromised if processes are not followed.

Certification and Approval

The idea of certification is much more predominant with legal frameworks for controlled e-voting than with uncontrolled e-voting. Often with voting machines, a certification organization is mandated to test equipment, verify its security features and allow, for instance, local governments such as those that operate in the United States, to rely on the expertise of external bodies about the reliability of equipment. Certification is also useful where electoral administration is decentralized and a variety of e-voting solutions may be adopted. In England, one of the recommendations coming out of the municipal election experiments with e-voting was to have a centralized certification body that could test and approve the systems before they get used (Electoral Commission 2007a). As Internet-based voting increases nationwide, there may be value in creating a dedicated Canadian certification authority that can assist lower-level governments and other organizations with certifying their electoral technology.

Third-party certification can act as a safeguard for authorities without the resources or expertise to conduct a full-fledged audit or internal review of an e-voting system. It can also serve as a means of due diligence for upper level governments that may wish to allow entities like local governments to use the system, while requiring local entities to choose equipment from an approved supplier. The US federal government relies heavily on certification and ties it to local election administrators seeking federal funding to purchase election equipment. The *Help America Vote Act of 2002* s. 231(b) directs the Director of the National Institute of Standards and Technology to evaluate independent non-federal laboratories and recommend them for accreditation by the US Election Assistance Commission (EAC) to certify voting machines. The manual produced by the EAC specifies in detail the procedural requirements that must be fulfilled for laboratory accreditation. Any laboratory that meets the relevant requirements can be approved for accreditation by the EAC. Individual states have the option of providing their e-voting machines for certification using EAC-accredited laboratories.

For Canada, requiring third-party certification could be an added measure of confidence that a system is ready to be used, but the same could also be completed by professional auditors or another independent reviewing organization. For example, in Estonia, the independent National Electoral Committee, consisting of two judges,

oversees elections, and an auditor (KPMG Baltic) oversees compliance and an independent programmer is hired to review source code. In New South Wales, the Electoral Commission may approve an e-voting system if a set of criteria are met, and there is a requirement that the audit result be provided to the electoral commissioner seven days before a vote (*Parliamentary Electorates and Elections Act 1912*, s. 120AD(2)).

Final third-party sign-off certification may not provide enough flexibility when a system requires dynamic tweaks to respond to hackers, but the notion that a system must pass a series of defined tests and a comprehensive assessment before each election still applies. Creating or appointing an independent entity with the ability to test and anticipate new threats is important.

We recommend that some governmental body, committee or external agency separate from the IT staff designing the system be required to certify or approve key components of the system prior to the use. The legislation may use general language such as requiring the electoral authority to appoint an independent, arm's-length and qualified reviewer before using the system in a general election.

Holding Cryptographic Keys

One of the most consistent means of ensuring secrecy of the ballot is using cryptographic technology. When a voter casts a ballot on their home computer, an advanced mathematical formula is applied to encrypt the information so that it can be securely transferred. In order to read the vote, someone must possess a cryptographic key with instructions to descramble the information. The votes are also stored at the centralized server in this matter, so that someone observing the server would be unable to decipher how a vote was cast until it was encrypted.

Most systems use technology analogous to a mail-in ballot, in that the vote is encrypted, this encrypted ballot is attached to a voter's identity, and then encrypted in an outer "sealed envelope" to allow secure delivery to prevent the vote from being manipulated along the way. The voter's information is stripped prior to the de-encryption codes known as "private keys" from being run.

The concern is that whoever possesses the cryptographic key has the theoretic ability to uncover the voting preferences of a vast number of voters if they were able to gain access to the area in which the votes are stored. This concern can be overcome by ensuring the private key is securely stored and by requiring more than one individual to access the key.

In Estonia, the private key is stored on a tamper-resistant hardware security module and protected by a multiparty authentication scheme. In order to access the private keys, a quorum of the National Electoral Committee is required to provide a password (Heiberg et al. 2011).

In Norway, the regulations require the key to be held by those with diverse interests. In order to satisfy this requirement, an electoral board is formed with 10 representatives of different political parties, each receiving a portion of the key (OSCE 2012b).

Switzerland, on the other hand, generated a key that was kept by the police agent, but which required two passwords, kept by a notary as well as two groups of election officials to unlock. New South Wales regulations allow the commissioner to appoint a five-person board to control the keys, and three keys must be present to open a ballot box (Brightwell 2011).

We recommend that the legal framework require that any cryptographical key be divided among a sufficient number of persons recommended by different political entities and that appropriate security steps be taken.

Division of Technical Activities

Similar to the distribution of cryptographic keys, it is important that sufficient checks and balances exist throughout the e-voting system to ensure that authority and capacity to make changes are widely distributed.

Electronic voting is inherently centralized, so the legal framework should require procedural decentralization and safeguards to ensure that no abuse is possible.

Additionally, the legal framework should not permit unilateral access to any critical component of the e-voting system and should ensure the system is designed so that there is no feasible way to determine how voters voted and that no partial report is available prior to the closing of the polls (Volkamer et al. 2011).

The division of technical activities should be handled both by technical measures as well as physical steps. In its pilot projects, Norway runs the vote de-encryption server in a different location from the vote-recording servers under different divisions of the government. Estonia runs each process on a different server, with different individuals tasked with the authority to run a process, so that there is both a separation of duty as well as a separation of critical elements (Volkamer et al. 2011).

Legislation, regulations or policy statements from the Chief Electoral Officer should ensure that voter secrecy is achieved through the division of technical roles, so that no individual can unilaterally access and manipulate processes or data.

Summary of Recommendations

A successful implementation of e-voting will require well-defined roles and responsibilities to ensure the system is secure and to provide the public with confidence that any negligence or mischief at the electoral authority cannot affect the accuracy of the votes or voter anonymity. The legislative framework should ensure that e-voting does not overly depend on any one individual or closely connected group. We recommend:

1. Some independent group with recognized technical expertise, internal to Elections Canada or external, should be required to certify and approve that a system is secure, reliable and ready to be deployed in a general election.
2. Roles should be assigned to determine if an electronic voting system's security, integrity or privacy has been breached.
3. Cryptographic keys should be divided among enough individuals, ideally representing different political parties, to protect voters' privacy and ensure votes are not prematurely de-encrypted.
4. A general division of technical roles and duties should be in place across the electoral authority to counter concerns regarding centralization and collusion and ensure that at least two unconnected people approve any changes.

Contingency Planning for Worst-Case Scenarios

While every reasonable effort should be made to design systems that will not fail, the legal framework must take into account the possibility that there will always be an element of risk. This could include an error in design and operation; outside sources of interference, such as power outages, that affect computer equipment; natural disasters; or attempts to hack into the systems or disrupt the vote.

It could be a very serious stain on the operation of Canadian democracy if failures or tampering led to the effective disenfranchisement of some citizens, which could alter outcomes or undermine public confidence in the process.

The legal framework to address breakdowns in the system should adopt procedures and regulations that ensure e-voting can be carried out in an efficient, prompt and trustworthy manner. The framework must also be flexible enough to adapt to future challenges.

Remedial Legislation for Emergencies

The *Canada Elections Act* provides the Chief Electoral Officer with a high level of discretion to ensure the smooth conduct of elections in the face of unforeseen issues. Section 17.(1) is particularly important, as it gives the Chief Electoral Officer the power to adapt any provisions of the Act in case of "emergency, an unusual or unforeseen circumstance or an error". If problems occur during voting that are not apparent until afterwards, s. 524 gives a court the ability to annul an election if "there were irregularities, fraud or corrupt or illegal practices that affected the result of the election".

Confidence in the legal framework will be increased if democratic debate can validate the procedures taken to respond to a threat, and Canadians can know in advance what steps will be taken to ensure the integrity of the election. Ideally, the legislation should provide some guidance on how the electoral authority should react to certain events, particularly where it may involve delaying or even cancelling e-voting.

One specific issue that is distinctive to e-voting is the potential for denial of service attacks. A denial of service attack is generally caused by a web server being deliberately overloaded by too many simultaneous requests, often the result of a computer virus that remotely controls thousands of computers and creates a heavy traffic load. This may result in a voting website being either slow or virtually inaccessible during an attack. A denial of service attack was the reported cause of delays in voting at the 2012 NDP leadership race, likely worsened by the short window of time allotted to voting.

Holding online voting well in advance of the day of the election is one way to mitigate this risk. This may be supplemented by allowing the electoral authority to temporarily extend the Internet voting period. Section 17.(3) of the *Canada Elections Act* currently sets conditions for when voting at a polling station may be extended, and a similar provision should exist for electronic voting. To be effective, any extension of e-voting as a result of a major disruption may need to be at least a calendar day to communicate to the electorate and give voters ample time to again attempt to vote.

In Estonia, a plan is in place to fend off potential attacks on the system conducted by foreign entities such as denial of service. In such a case, the electoral authority would block access to the e-voting system to anyone located outside of Estonia with the exception of voting conducted at embassies.

Sometimes it is not only real threats, but perceived or potential threats that can trouble voters, such as the possibility of their vote not having been cast or counted. Both Norway and Estonia permit a voter to cast an electronic ballot numerous times, with only the final ballot being included in the count. Provisions are also in place to allow a voter to cast a paper ballot, at which time all electronic votes cast by that voter are annulled. Without a legislative amendment, electoral authorities in Canada would be arguably unable to implement this change, as s. 7 of the *Canada Elections Act* prevents an individual from requesting a second ballot once they have already voted.

In the case of a system breach, Estonia's National Electoral Committee has the power to cancel e-voting and authorize voters to revote on election day (Canada–Europe Transatlantic Dialogue 2010). This general authority has been further defined by Estonian Bill 186, which would give the Electoral Committee explicit authority to suspend or terminate the electronic vote and to revoke all or some of the votes. In the case of cancellation of a vote, the legislation mandates that the Electoral Committee must immediately inform all voters who have voted online and make provisions for them to revote.

In Norway, the Data Protection Inspectorate, an independent state agency, implements the *Personal Data Act* and has authority to stop the election if personal data are improperly handled (OSCE 2012b). Likewise, article R176-3-3 of France's *Electoral Code* allows the office of electronic voting to permanently or temporarily stop Internet voting if its integrity, secrecy or accessibility is no longer guaranteed.

Lastly, if a serious vulnerability ever surfaces, a decision would have to be made as to whether to stop the online voting and whether the integrity of currently cast votes would be able to be maintained.

The electoral authority should establish protocols for determining if and when to shut down e-voting, under what conditions to extend voting and what plans are in place to ensure the integrity of the vote in case of a breakdown. Ideally, legislation should be amended to give the electoral authority explicit authority to cancel or terminate votes, as well as ensure that voters who cast their vote online are provided a sufficient opportunity to cast a paper vote in the case of any concern with the e-voting system.

Legal Status of Invalid Votes

In Norway's 2011 election, seven votes that were cast electronically returned erroneous results for unknown reasons. It is hard to determine sometimes whether this is an error in transmission or encryption, or whether it was an intentional effort by someone with the technical savvy to submit a digitally spoiled ballot. The Organization for Security and Co-operation in Europe thus recommends that a clear criterion be established in the electoral framework to determine the status of corrupted ballots and that procedures are updated to ensure timely detection thereof (OSCE 2012b). In Estonia, one invalid vote was submitted, but Estonian authorities did not undertake a comprehensive investigation to determine whether it was accidental or intentional, fearing it would create a negative precedent on breaking the secrecy of votes (Heiberg et al. 2011). Nonetheless, the legal uncertainty regarding corrupted votes has prompted legislative changes. New legislation in Estonia, Bill 186, treats all irregular votes as invalid.

For Canada, the legislation itself may need to define whether such erroneous ballots are presumed spoiled ballots or irregularities. The importance is not trivial, since irregularities under s. 524 of the *Canada Elections Act* would potentially lead to an election being overturned, whereas spoiled ballots would typically be excluded from the final count. The onus would be on those contesting the election to show an irregularity existed, but this may require technical experts to testify, which may exacerbate the tension that already exists "between allowing an application to contest an election on the basis of irregularities and the need for a prompt, final resolution of election outcomes" (*Opitz v. Wrzesnewskyj*, paragraph 47).

The current *Canada Elections Act* requires a judge conducting a recount to reject votes that have been marked in a way that contravenes the Act, but the legal status of digitally transmitted ballots may be unclear, as the Act does not address digital markings. The *Canada Elections Act* should be amended to provide more specific guidance than it currently does on whether an irregular electronically cast vote is invalid or may be considered an irregularity.

Judicial Recounts

The Council of Europe recommends that recounts be permitted. Currently s. 300 of the *Canada Elections Act* mandates that recounts happen in races where the margin of victory is less than 0.1 percent of the votes cast.

At least one Canadian jurisdiction has procedures for a recount when e-voting has occurred. Halifax prescribes that for a recount, the original file containing the encrypted votes is to be verified by an independent third-party expert and a judge then de-encrypts the votes and ensures that the total matched (Canada–Europe Transatlantic Dialogue 2010).

It does appear to be a sound general concept that whenever an official recount is conducted where e-voting was used, an expert third party should be available to assist the judge to verify technical issues, in addition perhaps to scrutineers from candidates who may also review the data. The *Canada Elections Act* currently allows a judge to retain support staff to assist in a recount. An independent technical expert can provide confidence that the counting is correct and that no data have been manipulated.

With voting machines in a controlled environment, it is often recommended that paper verification records be printed to ensure a recount can be conducted. With online voting, paper receipts are less feasible as the data will need to be de-encrypted before receipts can be printed. However, maintaining backups of the voting data on an unalterable medium such as a tape drive may be sufficient. Additionally, it may be possible to calculate

and record cryptographic algorithms alongside voting data that can be used to validate the integrity of the stored results. These mathematical constructs would provide a reliable level of certainty as to whether any electronic records have been accidentally or intentionally altered.

From a practical perspective, Parliament may wish to change the *Canada Elections Act* to exclude e-votes from the automatic recount provisions triggered by close election results. The rationale for automatic recounts is to ensure counting errors or misplaced ballot boxes do not affect close results. Those same concerns with human tabulation errors do not apply to e-voting. Requiring every judicial recount to independently verify e-votes without further evidence of irregularities or fraud may be inefficient and unnecessary. Ideally, it should be within the discretion of a judge whether it is necessary to independently verify the e-voting results. Similarly, anyone with concerns over the validity of e-voting could apply under s. 524 if there is concern with fraud or irregularities.

The legal framework for handling recounts should involve a combination of legislative amendments as well as regulations created by the electoral authority. The legislation should define under what circumstances e-votes should be recounted and require the electoral authority to create detailed regulations describing how a recount will be conducted. The electoral authority may require some flexibility in determining recount procedures, since the exact procedures will depend on the e-voting technology.

Planning for a High Level of Availability

The legal framework should require that electoral authorities develop a comprehensive plan to ensure that an e-voting infrastructure can withstand natural disasters as well as attacks. Electronic voting systems are required to be available at all times during an election, and they must be capable of withstanding attacks to both software as well as hardware. The security of a voting system needs to be considered in regard to how it isolates and reacts to failure (Alvarez and Hall 2008).

The importance of this is not trivial. The 2011 Breivik terrorist attack in Norway destroyed part of the building that hosted parts of Norway's e-voting system. The system should be designed with no single points of failure: "If failure in one part of an information system can cause failure in other interconnected parts, then the system is susceptible to cascade failure" (Hole and Neglen 2010, 22).

Under a paper-based system, widespread failure in Canada is unlikely because votes are stored and counted in 308 electoral districts, at various polling stations. While it is possible to host electronic voting in each riding, the technical expertise needed to monitor and scrutinize the system may make it unfeasible. It may be possible to have some modularity, such as dividing or replicating servers in various regions. Norway has a decentralized system in which various components of the voting system are stored in physically different locations under the control of various ministries. Geneva's system replicates voting data and saves the information in various locations. Decentralizing increases the amount of resources required to administer the system, but decreases the effectiveness of attempts to disrupt or manipulate electoral systems.

Electoral officials should be required to have full plans covering possible disruption scenarios. The New South Wales auditor report mentioned this as one of the few deficiencies in the state's planning (PricewaterhouseCoopers 2011). The Australian state of Victoria, currently working to deploy Internet voting, has embraced a best practices framework that involves conducting ongoing risk assessments and assessing evolving risks. The system must be deployed using failure-critical engineering practices that are auditable and transparent (Buckland and Wen 2012).

Currently, the Chief Information Officer Branch of the Treasury Board of Canada Secretariat has a number of guidelines on security available that could assist electoral authorities in developing a risk management plan. Such a plan should be tailored for the particularities of electronic voting, including high availability, absolutely no data loss or manipulation and the need to adjust to ongoing risks and other threats.

A clear disaster recovery plan should be created by electoral officials and updated before each election. They should ensure the system is fully redundant and modular where possible. Important data, such as stored votes, should be required to be stored in duplicate. All known risks must be identified.

Technical Co-operation

In addition to an internal plan to maintain the high reliability of an e-voting system, it is important that the legal framework provide the electoral authority the tools to collaborate with other government departments as well as third parties such as Internet service providers.

One of the key aspects of Estonia's success is that it has a highly integrated election process. Accessibility and authentication is very high because of the use of an integrated national ID card, which Estonians use for common tasks, including government services and even transit (Martens 2010). The use of the national ID card enhances voters' familiarity with the card and provides more confidence in the security measures when they use it to vote.

A second reason for the success in Estonia is the high level of co-operation in the protection of telecommunications infrastructure. As a response to an earlier attack on government infrastructure, Estonia now brings together telecommunications companies, IT staff and specialists from across the government to respond to any sort of threat. The National Electoral Committee, volunteers from an organization called the Estonian Defence League's Cyber Unit and others actively monitor Estonian web traffic for potential attacks or malware (Heiberg et al. 2011). Estonia has plans in place to disallow access to voting systems from outside of Estonia in case of a cyber-attack, allowing traffic from only embassies and trusted locations. The Organization for Security and Co-operation in Europe's report on Norway recommended that authorities collaborate with relevant agencies to provide monitoring and security during future elections (OSCE 2012b).

Canada's cyber security strategy in concept appears to recognize the need to bring together government institutions and the private sector to combat cyber security threats. However, this needs to be formalized for the specific risks that surface during an election to ensure that collective resources are brought together and are on standby 24/7 during the online voting period.

Electoral authorities should work closely with the Government of Canada's Computer Incident Response Team, computer security companies and Internet service providers to provide measures to check computers for viruses or potential malware that could affect computers used for voting, look out for systematic attacks and develop plans to combat possible electoral threats.

Summary of Recommendations

The *Canada Elections Act* contains some remedial language for reacting to worst-case scenarios, such as allowing the Chief Electoral Officer to adapt the Act in response to an "emergency, an unusual or unforeseen circumstance or an error" (s. 17.(1)) and permitting a judge to order a revote. Confidence in the e-voting legal framework will be increased if remedial contingencies for known electronic risks are included in legislation and clear disaster plans are implemented to detect and react to problems. The legal framework should ensure legislative certainty and finality of the results. We recommend:

1. Clear procedures should be created, preferably in the *Canada Elections Act*, for cancelling electronic voting, notifying voters and allowing recasting of votes if privacy, security or integrity has been unacceptably compromised.
2. The Act should list conditions under which officials may temporarily expand the online voting period if service is interrupted for more than a determined time.
3. Requirements in the Act and regulations should be in place on how to treat invalid votes and other irregularities.

4. Regulations should detail how electronic votes are handled during a recount, although we recommend that the Act provide judges with increased discretion as to whether e-votes should be recounted in the case of a close election result.
5. A clear disaster recovery plan covering all known risks of disruption should be produced before each election.
6. The government should ensure that a technical response team, including leading Internet service providers, other departments, and anti-virus and securities vendors, is formed to identify and respond to potential threats during an election.

Electoral Offences

Voting over the Internet provides new opportunities for individuals intending to disrupt or influence an election. While a system should be inherently secure, disincentives such as fines or imprisonment can be used to discourage fraud and other activities. The legal framework should ensure that foreseeable activities are prohibited. Only Parliament can create criminal offences, and legislative changes will have to be made to ensure that electoral offences cover Internet and electronic threats.

Influence while E-voting

Internet voting, similar to voting by mail, is potentially susceptible to coercion or vote buying when the voting occurs in an uncontrolled environment. The current election law requires anyone assisting another in casting a vote to mark the ballot as the elector intended and refrain from attempting to influence the voter in choosing a candidate (*Canada Elections Act*, s. 155). These provisions are broad enough that they should cover those attempting to influence a voter casting their ballot over the Internet. Parliament, out of an abundance of caution, may wish to add a provision to the *Canada Elections Act* to specifically make it an offence to influence a voter casting their ballot electronically.

Some jurisdictions have provisions to ensure that the design of e-voting software does not influence voters by benefiting one candidate over another. Switzerland's federal ordinance on political rights prohibits misleading or manipulative messages on a voting website (article 27*e*). The *Canada Elections Act* currently includes standards for ballot design. It may be possible to include the design of the e-voting ballots in the legal framework or require an e-voting software to randomize the order of names, although this is likely best left to the electoral authorities based on the capacity of the voting technology.

The *Canada Elections Act* makes it an offence for voters to show their ballot to prove how they have voted (s. 164(2)b). For the purpose of clarity, an amendment to the section could be made to ensure that it is also an offence to show reproductions (such as a video) of casting a ballot. Electoral authorities may also wish to have the voting software warn voters of any such offence. On the other hand, with the rise of social networks and photo sharing software, it may be futile to prevent individuals from sharing which candidate they voted for. A better solution may be to follow Estonia, which allows voters to change their vote online or by voting in person, thus rendering reproductions of a vote meaningless because the reproduction might not reflect the final vote.

The current punishment under the *Canada Elections Act* for offences under subsection 164(2) is imprisonment for up to three months in jail or a maximum fine of $1,000 or both. Halifax's bylaw sets a higher $10,000 for influencing a voter in a municipal election.

We recommend that the Act impose a higher punishment for attempting to influence a person e-voting.

Secrecy of Electronic Ballots

Current law requires election officers, candidates and candidate representatives to maintain the secrecy of the vote (*Canada Elections Act*, s. 164). Furthermore, anyone assisting another in casting a vote is prohibited from

disclosing how that person voted (s. 155). Section 164, however, does not refer to technical staff or vendors who potentially have access to voting data.

New South Wales introduced a provision aimed at e-voting whereby any person who becomes aware of how an eligible voter voted is not to disclose it (*Parliamentary Electorates and Elections Act 1912*, s. 120AG(1)). The law requires any technical staff or individuals working on the system to sign a form acknowledging that they are aware of the offence.

Another area of concern regarding the secrecy of the vote is that some workplaces and computers may have software installed that allows systems administrators to observe computer activity, including for legitimate purposes such as providing technical support. Reasonable steps, including warnings, should be taken to protect a voter's privacy in this regard.

We recommend that Parliament broaden s. 164 of the *Canada Elections Act* to ensure that individuals such as third-party contractors or companies monitoring workplace computers maintain the secrecy of the vote and take reasonable steps to ensure they do not accidentally observe someone voting using a monitored computer.

Hacking or Disrupting the E-voting System

Electronic voting is more vulnerable than traditional voting to widespread, systematic attacks. The most common threats are those actually attempting to break into the system, as well as "denial of service" attacks (as mentioned above) that try to discourage people from voting by overloading servers with fake requests.

Traditional offences under the *Canada Elections Act* include the use of forged ballots, ballot box stuffing and ballot destruction (s. 167). The maximum penalty for violating s. 167 on conviction on indictment is a $5,000 fine, five years in prison, or both.

Prior to using Internet voting, New South Wales created a specific offence with a fine or imprisonment for up three years, or both:

> A person must not, without reasonable excuse, destroy or interfere with any computer program, data file or electronic device used, or intended to be used, by the Electoral Commissioner for or in connection with technology assisted voting. (*Parliamentary Electorates and Elections Act 1912*, s. 120AI)

It should be an electoral offence either to interfere or attempt to interfere with any software or hardware used for electronic voting, enforced with severe fines and potential for imprisonment. Electoral officials should create regulations and policies to facilitate legitimate testing of electoral technology.

Spoofing and Misinformation

One of the concerns with e-voting is that "spoof" voting websites or emails that pretend to originate from Elections Canada may confuse voters and potentially mislead them into thinking they voted.

Current electoral law in Canada prohibits printing a ballot or what purports to be a ballot at an election with the intention of causing the reception of a vote that should not have been cast or the non-reception of a vote that should have been cast. The manufacture of ballot boxes with hidden compartments is also prohibited (*Canada Elections Act*, s. 126).

There is currently no offence for creating a fake voting site. It would undermine the confidence in the electoral system if individuals were able to create fake voting sites or to knowingly distribute links to such sites with the intention of misleading voters.

It should be an electoral offence to wilfully create or distribute to the public communications including websites that may mislead voters. Election officials may also consider providing a method for voters to confirm their votes were counted.

Submitting Corrupted Ballots

Someone intent on disrupting an election may not need to actually affect a vote, but may attempt to create the perception that there is a problem with the voting system. For example, one of the concerns is that it may be possible for a voter to knowingly alter a voting program on their computer to submit a false voting result. Similar to spoiling a ballot, it is possible for sophisticated computer users to alter their ballot so that it may be unreadable by vote tabulation software. It is foreseeable that a piece of software may be distributed alongside an election, potentially resulting in numerous erroneous ballots. Section 167(2) of the *Canada Elections Act* makes it an offence to alter, deface or destroy a ballot or put a ballot into the box other than prescribed by the Act.

Our research did not identify legislation elsewhere that treats knowingly submitting a corrupted ballot over the Internet as an offence. A court in Estonia ruled that a voter who intentionally corrupted his ballot was not entitled to challenge the voting results, but there was no deterrent available to prevent him from submitting fake ballots in the first place.

Whether or not this should be an offence is debatable. Some may argue that the right to spoil one's ballot is a form of freedom of expression, and in addition the right to a secret ballot makes it very difficult to prove electoral offences without violating the secrecy of the vote. Others may argue that any action designed to undermine voter confidence in an election is a reasonable limit. This may include distributing software designed to help voters create a corrupted vote.

As long as it remains an offence to submit a spoiled ballot, even if it generally is impossible to enforce, the *Canada Elections Act* should be adapted to apply to a wilfully corrupted electronic vote.

Unauthorized Disclosure of Source Code

In section 0 of this paper, we recommended that electoral administrators implement a framework by which scrutineers, academics or other observers may be given access to the source code of the voting system. If a decision is made to not publicly distribute the source code, disclosure could be prevented by either contractual or legal measures. Estonia uses non-disclosure agreements to protect its source code. New South Wales, on the other hand, has a specific provision prohibiting the release of source code or software lists unless done under an authorized procedure. The latter makes it easier to modify terms of disclosure or create policy provisions governing the disclosure.

It should be an electoral offence to publicly distribute source code or other proprietary election information not being in accordance with authorized procedures. The Chief Electoral Officer or an authorized entity should create subordinate regulations or procedures to govern access and disclosure.

Summary of Recommendations

The *Canada Elections Act* contains a list of offences, cast in general terms, that may not be sufficiently broad or clear with respect to conduct that specifically concerns e-voting. In order to ensure legislative certainty and discourage disruptions to the electoral system, legislation should be passed to forbid attempts to abuse the e-vote system. Additionally, the potential for creating widespread voter fraud affecting multiple electoral districts should be taken into consideration in determining appropriate sentences or fines. We recommend:

1. Fines and penalties associated with voting offences, including influencing the vote, should be increased.
2. The *Canada Elections Act* should make it an offence for all technical support staff, vendors and anyone who may have access to the system to violate the secrecy of the vote.
3. Employers (and others) who use screen capture technology or other methods to observe their computers should be required to take reasonable steps to ensure the secrecy of the vote, including alerting employees.

4. Stiff penalties and specific offences should be created for attempts to systematically affect the vote, including disrupting election servers, manufacturing vote-altering software and interfering unlawfully with any electronic voting equipment.
5. The Act should ban wilful creation, promotion and linking to spoof election sites that could lead someone to wrongly think that they have voted.
6. The Act should make it an offence to wilfully corrupt and submit an e-vote.
7. Legislation should prevent unauthorized disclosure of e-voting source code.

Technological Standards and Consultation

One of the challenges with formulating a legal framework for e-voting is that the framework needs to be flexible enough to adapt to improvements in technology, while meeting minimum standards such as ensuring the integrity of the vote, protecting voters' secrecy and responding to disasters. The framework should require that a technologically robust solution be in place before an electronic voting system is used in a real election.

While electoral legislation may set minimum standards, most of the practical technological decisions are best left to the discretion of the electoral authority, and contained in regulations, requests for proposals, technical plans and other administrative documents. Generally, the legal framework should be technologically neutral so as to ensure the best technology available can be chosen. However, with certain technological choices, there may be a need for a broader consultative process built into the framework or even specific legislative choices made by Parliament.

Requests for Proposals and Consultation

While the electoral authority may determine many of the technological standards, the legal framework should require a broad level of technical consultation before the final e-voting solution is determined. The consultation should provide an opportunity to create contractually binding requirements that can be scrutinized by the public prior to implementing e-voting. There are two primary ways in which the technical consultation can occur.

Consultation can occur prior to finalizing the technical specifications. Estonia, as one of the early leaders in e-voting, undertook a series of consultative efforts before developing the software. Estonia originally developed its system primarily in-house with the assistance of third-party software developers, but based it on detailed technical reports, threat assessments and requirements that were formed in collaboration with academics, experts and political parties. The resulting technical documents contained many specific design elements, security requirements and procedural standards (Estonian National Electoral Committee 2004). The National Electoral Committee uses these as the basis for auditing the system to ensure compliance.

A second way of conducting consultation is to incorporate consultation directly into the request for proposal and bidding process before choosing a software developer to create the e-voting system. This was the process undertaken by Norway. Prior to issuing a formal request for proposal, Norway's electoral authority initiated a six-month competitive dialogue with companies and consortiums to improve project specification before leading to a full tender (OSCE 2012b). As a result, software developers and the public were able to provide feedback on the detailed technical requirements. A technical specifications document is publicly available (Norwegian Ministry of Local Government and Regional Development 2009).

Whether the e-voting system is developed in-house or sent out to tender in a competitive bidding process, the legal framework should require a transparent consultation process before the technological specifications are finalized.

Permitting Voters to Recast Ballots

While many implementations of e-voting are generally very similar, there are certain key technological choices that should be debated by Parliament before they are adopted in the legal framework. One of these is whether to allow voters to change or update their vote once it has been cast online.

In Estonia, voters may submit more than one e-vote, with the system designed to count only the final vote. Earlier votes by the same voter would be purged before votes were unencrypted to ensure the privacy of each ballot. Voters who are concerned that their computer may have been hacked can revote, as can someone who felt pressure to vote a certain way. Voters can also override their vote by voting in person at an advance poll.

Vote updating is seen as a measure to establish trust regarding the integrity of a published result (Volkamer et al. 2011). This would likely require a change of the *Canada Elections Act*. Additionally, the software must be able to purge redundant votes. Overriding a previous vote could be done unlimited times, as in Norway and Estonia, or conditions may be in place to do so only once at an elections office.

While vote updating is a valuable tool that can be used to alleviate concerns with vote buying or computer problems, it would be a new concept in a Canadian election. As such, there may concerns with whether voters who vote online are given an advantage over voters who vote by paper.

While vote updating may raise concerns with whether voters are treated equally, a court in Estonia found that vote updating was a legitimate infringement on the right to equality. A legal challenge was submitted to Estonia's Supreme Court on the grounds that there was a principle of uniformity that was violated if electronic voters could cast a ballot more than once (*Constitutional Judgement 3-4-1-13-05*). The president argued that the constitution required votes be cast only once and that every voter be given an equal opportunity, and as such not all voters had the opportunity to change their vote. The court rejected the principle of absolute equality, finding that modernization of electoral processes was a legitimate infringement of the right to equality and principle of equality (paragraph 26). The court found that vote updating was an appropriate means to protect the freedom of elections and secrecy of voting against outside influences, which previously was guaranteed through the privacy of a polling station (paragraph 32).

In our opinion, voter confidence in Canada would be increased if the legal framework could permit voters who cast their ballot online to update their vote either online or in person at a poll. However, this should be debated further by Parliament.

Receipts and Voter Verification

A second technological choice that requires more extensive debate and consultation is whether voters should be permitted to verify that their vote counted. Not every jurisdiction permits voters to verify their vote, and new methods of verification are emerging. The legal framework may have to be adapted in order to accommodate this. The primary method used to allow voters to verify their vote is though the use of a voter receipt. A voter receipt is a code confirming to a voter that their vote has been counted and, in some cases, demonstrates a vote has not been manipulated. The voter receipt would remain private unless the voter chose to share it. Some require cryptograph proofs to connect it to a vote.

There is currently no functional equivalent to a voter receipt in Canada, as a paper-based system cannot ascertain whether a vote was accurately counted or spoiled, although it does allow for recounts. This was a major issue in the 1995 Quebec referendum, when it was found that in some polling districts in non-francophone ridings over 50 percent of the ballots were rejected (Shaffer 2008).

Voter receipts are a confidence measure designed to assure voters the system has worked, although it is unclear what the remedy would be if a voter claimed the vote in the system did not reflect the one they cast.[11]

Whether a voter receipt is valuable or necessary is debated. Depending on how a voter receipt is designed, it may allow voters to prove how they voted, which may open the door to vote buying. Some have claimed receipts provide a false sense of verification (Open Rights Group 2007). Others claim they are necessary to create an audit trail that is verifiable (Goldsmith 2011). Some systems allow a voter to confirm their vote on the final tally, although there is a risk that this could be used by voters who sell their votes to prove how they voted.

A 2006 Dutch election provided voters with a candidate code they entered in voting, and a technical code that they later received. With both pieces of information, a voter could confirm how they voted. The election authorities "effectively opted to surrender protection against coercion of a voter in favour of greater transparency" (OSCE 2006, 15).

Norway, in order to provide end-to-end verifiability, created a system where a voter received a secret return code via text message after voting so they could verify their vote was counted as cast, although this was not provided in the final count (OSCE 2012b). Alternative means have also been tried to allow voters to verify their vote. Swindon, one of the English municipalities experimenting with Internet voting, allowed voters to enter a secret word that could be cryptographically connected to their vote (Open Rights Group 2007).

Estonia did not allow receipts in any of the previous elections, although Bill 186 proposes to allow voters to verify that their vote has been cast in future elections.

A voter receipt is one of the areas where there is a potential for values to conflict, possibly pitting having a transparent and verifiable election against the absolute secrecy of a ballot. At this early stage, this may be an area that deserves more public consultation. We recommend that the *Canada Elections Act* allow, although not require, election authorities to issue regulations detailing how voters can confirm their vote is counted.

Casting Blank Ballots

One of main differences between a paper ballot and an e-vote is that under a paper system, voters can easily reject or spoil their ballot. Whether the legal framework for e-voting should allow voters to spoil their ballot will likely need further debate and consultation.

One of the advantages of Internet voting is that it eliminates the subjective role of returning officers in rejecting spoiled ballots that may have been accidentally or intentionally marked in a non-prescribed way. This, however, may not satisfy those who reject or spoil their ballots in protest.

The Council of Europe recommends that the "e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote" (COE 2005, 10).

Not all implementations have permitted this. Estonia's voting software did not provide the option to cast an empty or blank ballot (Heiberg et al. 2011). On the other hand, Norway provides the option to cast a blank vote at the end of a ballot (Barrat i Esteve et al. 2012c). Halifax's request for proposal for potential e-voting vendors also mandated that the process include an option to provide a blank vote.

It is possible that a future court in Canada could find that the constitutional right to vote includes the right to cast a blank ballot; however, the current jurisprudence does not appear to be determinative. At the very least, the failure to provide voters an option to cast a blank ballot may serve as an incentive for individuals to attempt to use technological means to submit corrupted votes.

---

[11] Canadian courts have upheld that it would be inappropriate to ascertain how a voter actually voted under the principle of secret voting (*Wrzesnewskyj v. Attorney General (Canada)* 2012 ONSC 2873, paragraph 34 and *Cusimano v. Toronto (City)*, 2011 ONSC 2527).

While more debate may be warranted, we would recommend that the legal framework permit the electronic voting system to record intentionally blank or spoiled ballots.

Summary of Recommendations

The legal framework for e-voting should give the electoral authority a high degree of flexibility to choose the most secure technology, work on cost-effective solutions and deliver accurate results. Legislation should generally be permissive to allow new technology as long as it is secure, accurate and protects voter anonymity. A consultative process may be set up to ensure that the best technology is chosen. However, the choice of technology may also depend on certain functionality and features that may require trade-offs, such as between transparency and absolute secrecy. In those circumstances, legislative amendments and parliamentary discussion may be required. We recommend:

1. A transparent consultation process should be in place before technological standards or requests for proposals are formalized.
2. Parliament should discuss allowing voters to update or recast their e-ballot.
3. Officials should be permitted to introduce additional technology, including voter receipts or advanced authentication methods, if they are satisfied that it will increase integrity without disproportionally affecting the privacy of the voter.
4. Voters should be permitted to cast a blank ballot.

Testing and the Integrity of the Vote

Public confidence in e-voting will depend on what measures are taken to ensure that votes are accurately recorded, transmitted, received and counted. While there is legally a presumption of regularity in elections in Canada (*Opitz v. Wrzesnewskyj*), the less transparent nature of elections conducted using distance technologies likely means that the public will not be easily satisfied with a mere presumption of evidence, rather than solid evidence that the system is working properly. The legal framework should ensure there are credible and transparent measures in place to verify and document that the e-voting system is working properly.

Pre-deployment Testing and Implementation

In pilot projects conducted in England, one of the biggest criticisms was that local authorities allowed only six months between deciding to conduct a pilot project and election day. This did not allow sufficient time for planning and testing the e-voting solution (Electoral Commission 2007a).

It is important that any testing, if open to the public, be conducted only when full security measures and functionality are in place to avoid creating confusion or any impression that the final system may be flawed (Volkamer et al. 2011). An example often used by those who oppose Internet voting is an attempt to use Internet voting for an election in Washington, DC. Organizers challenged the public to attempt to hack into the system, which was successfully done by a team from the University of Michigan. The team managed not only to alter the votes, but also manipulate the system and even accessed video cameras located on the same computer network (Wolchuk et al. 2012). The system was not a typical Internet-based voting system where a user logged into a website to vote, but was designed so voters could upload a ballot they filled out in Adobe Acrobat to the server. The hackers found that by changing the file name, they could run system commands and the administrators had not even changed the default system passwords. While an independent security review may have identified many of these problems, the public release of a pre-election test proved to undermine public confidence and Washington did not proceed with Internet voting.

Where jurisdictions have implemented extensive pre-election testing by independent experts, the elections have gone far more smoothly. New South Wales had an independent auditor perform penetration tests, programming code testing, cryptographic testing and infrastructure security tests before the system was

permitted to go live. The New South Wales auditor, however, recommended that the regulations require clear criteria for tests to be conducted before a system is used in a real election (PricewaterhouseCoopers 2011).

In order to ensure that an e-voting system is secure, the legal framework should require the electoral authority to establish a set of procedures and tests that must be completed before a system is able to go live. These procedures should be updated before each election to ensure that the system is protected against new threats or vulnerabilities.

Accessibility and Usability Testing

One of the rationales behind using Internet voting is accessibility. The legal framework should require accessibility and usability tests to be conducted before each election. For best results, users, including those with disabilities, should be involved in both the design as well as testing of the equipment (Goldsmith 2011).

One of the common usability recommendations is that voters should have the ability to interrupt their voting prior to submitting their ballot and continue at a later time. A voter should also know clearly if a vote has actually been submitted by the system and received by the election authorities, and there should be no ambiguous steps in the process.

Also, the importance of proper instructions cannot be overstated. An election in Finland using controlled e-voting was annulled after a high number of electronic ballots were never submitted due to erroneous instructions that did not instruct a voter to keep their voting card inserted until after a final confirmation screen was shown. An administrative court ruled that instructions that were sent to voters did not clearly state that a secondary confirmation screen had to be clicked and the court ordered the election to be repeated (KHO:2009:39).

Sufficient usability tests are needed to ensure no one is accidentally disenfranchised. Accessibility should not be an afterthought, as it may also be related to security features. The less secure and controlled, the more accessible a system may be (Goodman et al. 2010).

Prior to use in a general election, extensive tests involving disabled voters, seniors and non-technical voters should be conducted using the voting system to ensure usability. The electoral authority should create procedures outlining how it will conduct these tests.

Physical Security Requirements

The legal framework should include provisions for physical security. This may include stating who has access to server equipment and under what conditions during elections. The general concept should include at least a two-person rule, where at least two individuals must be present to access any hardware or system component during an election or to make a software change (Electronic Frontier Finland 2009).

There are a variety of security measures and regulations. In the Indian state of Gujarat, regulations require that three smart card holders be responsible for starting and stopping the polls, and the data centre must be physically unplugged from the Internet prior to the beginning of voting (*Urban Development and Urban Housing Department Orders*).

Norway increases physical security by dividing critical elements among various governmental departments to ensure that system components are isolated from manipulation. Estonia has two government departments overseeing security and an auditor is present during the election to observe compliance (Electronic Frontier Finland 2009). Estonia also videotapes all system activity, as an added security measure, so that any unauthorized physical access to the system can be identified.

The regulations should detail steps to ensure that physical equipment is secure and to ensure that no individual can make unilateral modification to the servers or software during an election.

Permanent and Auditable Record Requirements

One of the primary arguments in favour of using only paper ballots is that physical records exist and they are harder to manipulate. The legal framework should require an equivalent ability to ensure e-voting records are not manipulated.

The discussion regarding voting in a controlled environment often leads to mandating paper receipts that can be counted afterwards. In the United States, there is a requirement that voting machines print a paper copy as an audit record, although this practice is not always reliable, as some machines leave a paper receipt but do not provide voters with the ability to verify it (Jones and Simons 2012).

Paper backups in an Internet system are not common, since the votes could be modified before they are printed. New South Wales requires printed copies of each vote, although they are printed at the close of online voting.

While a paper record is an easy means of preserving audibility, cryptograph verification may allow third parties to develop auditing mechanisms that are just as good or better (Alvarez and Hall 2008). Cryptograph logs make it nearly impossible to alter a record, as a math formula ensures that no data have changed.

Various countries use different methods of creating an unalterable record. Estonia backs up its voting data on tapes, which unlike hard drives cannot be rewritten (Martens 2012). Geneva, Switzerland, uses multiple servers and storage to prevent unauthorized manipulation, storing each vote cast on three different servers to protect against loss or potential manipulation of data (Chevallier et al. 2006).

Technical measures should be put in place to record all voting-related activity, including threats, disruptions, system failures, votes cast and invalid votes. It is important that the records be treated as a critical system, and like the votes, be incapable of alteration. This could involve writing logs directly to unalterable tape systems or using cryptographic technology to encrypt log files.

The legal framework should require that an auditable and unalterable record be produced, but the exact format should not be restrictively prescribed, as to allow flexible uses of technology to ensure the integrity of the ballot.

Verification of Results and Auditing Procedures

The *Canada Elections Act* already requires post-election reports be provided to Parliament and also mandates recounts in close contests, as discussed earlier. However, as online voting is fairly new and voter confidence in the system may be tentative, additional auditing and verification procedures may be incorporated into the legal framework to increase voter confidence.

Many jurisdictions require some form of audit to be released after an election, in addition to preliminary security, although the exact form and nature is often open. Estonia has an outside auditor conduct a procedural audit, to report whether IT staff and others have followed the procedures. New South Wales election law (*Parliamentary Electorates and Elections Act 1912*, s. 120AD) requires test votes to be tested and audited. Switzerland requires its system to be auditable as well.

The Council of Europe recommendations include ensuring the system maintains an accurate time source so that audit trails and observation data can be subsequently examined (COE 2005, recommendation 84). The Council also recommends that auditing information not be disclosed to unauthorized individuals and that all auditing steps taken be capable of preserving voter anonymity (COE 2005, recommendations 105 and 106). The rationale for this is that while primary security features should be made public to ensure confidence, secondary auditing procedures may be more secretive to make it more difficult for a potential hacker to avoid detection. It may even be prudent to have the auditing and recording technology designed by a different entity than those that develop the voting technology.

We recommend that sufficient auditing procedures be required to be conducted regardless of whether or not there is evidence of mischief. Some of the technical details of how they work may not be fully disclosed to the general public so as to make it more difficult for hackers to avoid detection.

Destruction of Voting Data

Electronic votes using cryptographic technology are highly secure and could take years to break without de-encryption keys. However, it is still foreseeable that the data could eventually be de-encrypted if the voting records were retained. The legal framework should require comprehensive regulatory procedures describing how voting data will be destroyed, as well as a time period for the retention. There was some criticism in an English municipal election because the data were kept on suppliers' servers for nearly a year after the vote (Open Rights Group 2007).

Estonia goes further than just stipulating that the data must be deleted. The country has internal procedures in place to physically destroy all media (such as hard drives or tapes) on which voting data are stored once the period for election appeals has ended (Martens 2012). Additionally, as with other procedures, an auditor is present to ensure compliance (Heiberg et al. 2011). Draft legislation (Bill 186) in Estonia proposes mandating the destruction of all election data within a month of an election, but not prior to the exhaustion of all appeals before the courts.

The legal framework should require the electoral authority to fully destroy any electoral data after a fixed period, once all rights to recounts or appeal of election results have occurred. The regulations should also require appropriate oversight to ensure that the data retention and destruction procedures are fully complied with.

Summary of Recommendations

To ensure the votes are accurate and the e-voting system is secure, the legal framework should require extensive testing at all stages and specific security steps. Ideally, minimum requirements would be in legislation and the electoral authority would be tasked to create detailed regulations and procedures. We recommend:

1. Regulations should clearly describe the tests that ought to be conducted prior to e-voting deployment.
2. Tests of the software should be completed to ensure it is accessible and usable. Disabled voters, seniors and other groups should be involved in the testing.
3. Regulations should require that physical security measures be in place to ensure the integrity of all equipment and prevent unauthorized access during an election.
4. Legislation should require auditable and unalterable records of voting activity, threats, disruptions and system activity. The electoral authority could create procedures that include unalterable tape backup and cryptographic encryption of logs.
5. Sufficient auditing procedures should be required post-election, even if some details of the audits remain confidential.
6. Procedures and timelines should be prescribed for destroying all voting data once all appeals are exhausted.

Controlled E-voting

Many of the considerations for developing a legal framework required to implement e-voting in an uncontrolled environment apply to e-voting in a controlled environment. In both cases, there should be strong requirements for security and integrity of the vote, and the *Canada Elections Act* should be amended to cover offences such as hacking.

Generally, when voting is used in a controlled environment, concerns will arise with storing and testing the individual equipment, since each terminal could be subject to manipulation or malfunction, and a single faulty

terminal could unknowingly affect the results of a number of voters. In Canada, where a voter generally only has to mark one choice (rather than vote in races for many different offices or rank candidates in order), the incremental value of controlled e-voting as opposed to paper balloting at an official station would be quite limited, whereas the cost per polling station would be much higher. Controlled e-voting machines can be expensive to purchase, and can also be expensive to securely store. As such, we cannot generally recommend a broad usage of controlled voting, particularly if it was to be used as an alternative to paper-based voting on election day as is done in some US jurisdictions and countries such as Brazil, India and Venezuela.

While we have focused the bulk of this report on Internet voting, we can envision some limited uses of controlled e-voting.

Uses of Controlled E-voting

Technically, a controlled environment for e-voting would include any computer or device provided and maintained by the electoral authority. This could include assisted voting devices as were tested in a recent Winnipeg North by-election, as well as computer stations that may be set up by the electoral authority to allow voters to use Internet voting.

In the United States, the *Help America Vote Act of 2002* mandated that every polling station have at least once one direct-recording electronic (DRE) device at every polling station. This provision is supposed to help voters with disabilities navigate the complex US ballots. A DRE is essentially a stand-alone electronic device that produces a paper receipt documenting how voters vote. Each state is able to independently set its own technological requirements, although many states follow the Voluntary Voting System Guidelines, recommended by the US Election Assistance Commission (US EAC 2005). The Voluntary Voting System Guidelines provide very useful standards on how to ensure that the controlled voting systems are secure and also minimal standards of accessibility for disabled voters. For any electoral authority planning on rolling out controlled voting for use at a poll, the Voluntary Voting System Guidelines should be an essential resource.

While specialized voting kiosks could be used to assist visually impaired or other disabled voters who want to cast their vote without relying on a third party, the high cost of running the tests in Winnipeg North do not make this the most efficient way to accommodate disabilities. Alternatively, an Internet voting system can accommodate most disabled voters without requiring these voters to come to a polling station.

On the other hand, the electoral authority may wish under certain circumstances to maintain an Internet-connected computer that could also be classified as a controlled e-voting machine. While these may function in the same way as a home computer, the legal framework would have to take into account that multiple voters would be using the same system, and as such any fraud or manipulation of the device could affect numerous voters. The electoral authority would be liable for ensuring the integrity of these computers.

There are a few examples of using controlled voting in combination with an Internet vote. For instance, the Australian military used e-voting for a limited test run in 2007, which was used on special voting terminals for military voters, but was discontinued due to the high cost of the system versus the low number of potential users (Australian Electoral Commission 2008). The Indian state of Gujarat also used limited kiosks for e-voting alongside remote voting, but very little academic literature has emerged from this experience.

The electoral authority in Canada may wish to maintain a limited number of controlled voting stations to use in special contexts. These could be used as an alternative for some special ballots, for absentee voters who have limited access to mail or for voting that takes place in locations that are secure and controlled. The two most obvious groups of users would be military voters deployed abroad as well as eligible voters in penitentiaries. Both of these groups may have limited access to their own Internet-connected computer, and so a number of voters may need to share a terminal.

Other possible locations for controlled e-voting are Canadian embassies, high commissions and consulates located abroad. This may be essential in countries where an embassy may be the only location where encrypted votes could pass a national firewall.

Domestically, the electoral authority may wish to set up an e-voting terminal in areas where there may be a high proportion of out-of-district or absentee voters. Possible locations include universities where students who live on or near campus may be eligible to vote for candidates in their home riding. Additionally, many voters who are out of district may choose to vote at any time at any returning officer's office.

For disabled or homebound voters without Internet access, there is the potential that an elections official would bring a cellular or satellite connected portable computer to their homes to assist with voting. This is already allowed in conjunction with paper ballots under s. 243(1) of the *Canada Elections Act*. An amendment to allow a voter to opt for similar assistance using e-voting may be considered.

In order to maximize the potential of any Internet voting in a controlled environment, the electoral authority may choose to provide voters the ability to register for e-voting at the location. For instance, a deputy returning officer or authorized official could check ID and authorize an e-voting account.

Provisions should be added to the *Canada Elections Act* to accommodate limited usages of Internet voting in a controlled voting environment.

Testing Controlled E-voting Devices

In order to use Internet voting in a controlled environment, the legal framework should include requirements to ensure the security and integrity of the devices that will be used for voting. This is especially important because unlike when voters e-vote over the Internet from home, in a controlled environment, voters will not have the opportunity to verify the integrity of the computers that they use. A compromised device could affect a large number of votes, and each device would not have the same level of oversight as the centralized servers on which the main voting software is run. In a controlled environment, the responsibility for ensuring unaltered software is installed is in the hands of the elections officials in charge of the device. This applies whether the voting device is an Internet-connected voting station or a stand-alone kiosk.

While it is important to have independent experts test the security of the code, it is equally important to ensure that devices used in voting are running the correct software. The legal framework should require procedures to test and ensure the validity of equipment, which is essential to ensuring that malicious software has not been installed.

In California, the secretary of state retains a copy of the source code and has the right to perform tests on voting systems (Hall 2006). Other jurisdictions require random tests of machines to ensure no equipment has been modified. Equipment testing may be done based on random polls from each district, fixed-percentage audit models that mandate a portion of stations be tested or adjustable-percentage audit models that require a greater number of tests in districts with close victories (Hall 2006). The importance of testing the equipment is high, because one malicious machine can manipulate a number of votes. It is also important because threats to controlled system may also come from outside the voting software, such as other parts of the system (Smith 2006).

If the controlled voting is Internet-based, then steps should be taken to ensure the software installed on it is the same as that installed on any other system. Appropriate procedures and hardware tests should be conducted to ensure the system cannot be modified and there are no accessible user ports on which malicious software could be installed. The exact steps to secure the system are best left to the electoral authority.

Different procedures may be required for stand-alone kiosks, since the results may be stored locally and the same central oversight is not available. Many stand-alone machines rely on proprietary source code. In such cases, the electoral authority should have full access to all software and code and be able to have it

independently verified. A number of Quebec municipalities also used electronic kiosk voting in local elections between 1995 and 2005, but these were discontinued after the Chief Electoral Officer raised concern that the e-voting software was not being independently tested, and the legal framework did not include adequate provisions for swearing in technical staff and testing voting equipment (Elections Quebec 2006).

We recommend that before any controlled voting system is used in an election, regulations are in place requiring an extensive testing regime and that the electoral authority develop procedures for testing the integrity of the voting systems before and after the election.

Summary of Recommendations

The electoral authority may seek to deploy an e-voting system in a controlled environment to facilitate accessibility and accommodate more voters. These may be stand-alone e-voting devices used for voters requiring assistance or secure Internet connected systems running the standard e-voting software used by remote voters in an uncontrolled environment. We recommend:

1. Legislation should permit electoral authorities to host controlled e-voting for military voters; voters in penitentiaries; overseas voters at embassies, high commissions and consulates; domestic voters in locations such as the offices of the returning officer; disabled voters in the home; and voters on post-secondary campuses, where absentee ballots are common.
2. Regulations should require e-voting devices to be tested before and after elections.
3. The electoral authority should have access to all software and code installed on machines.

Further Consideration: Specialized Oversight of E-voting

In our opinion, the current electoral system, with well-defined provisions in the *Canada Elections Act* and administered by an independent Chief Electoral Officer, is generally effective. Elections Canada has worked hard to protect the integrity and fairness of the system, even if it has required challenging the governing party.

While the administration is technically centralized, with the Chief Electoral Officer being given wide discretion to implement ad hoc rules under the *Canada Elections Act* in the event of unforeseen circumstances, this authority appears to be prudently used. The broad discretion is somewhat limited by the decentralized and distributed process of casting and counting ballots in Canada. Most Canadians vote directly in their electoral district and votes are counted directly at thousands of polling stations across the country. If there are problems with voting, or allegations of fraud, it is likely to be confined to a single electoral district.

Internet voting, however, generally necessitates a centralized ballot-counting process in which fraud, disruptions and even a system shutdown could affect some or all voters who intend to cast an online ballot. Under the current electoral structure, the Chief Electoral Officer would retain the sole discretion on how to react to emergency situations and major problems. In comparison, some other jurisdictions rely on electoral committees with judges and senior bureaucrats to make major electoral decisions. Even in Canada, tribunals and decision-making panels rather than individual administrators often make major regulatory and legal decisions. For instance, three judges will often decide on legal appeals at a provincial level and up to nine judges may hear major decisions at the Supreme Court of Canada. If a major e-voting incident occurred, would Canadians be confident in the decision of a single official?

The first deployments of Internet voting in other jurisdictions have mainly occurred under the same electoral structure as paper votes, with little institutional changes in place to accommodate them. However, recently, the trend has been to move toward specialized oversight.

In Estonia, the elections are administered by the National Electoral Committee, which is composed of members of the judiciary as well as high-ranking heads of various government departments. This committee has the authority to allow or shut down the e-voting system and invalidate all or a portion of results (Heiberg et al.

2011). The use of judges on the oversight body likely provides additional legitimacy and oversight, particularly within an emerging democracy. However, there was no requirement that any of the members possesses any special technical expertise. Most of the practical administration and development of the elections has come from the IT department. The Organization for Security and Co-operation in Europe had previously criticized this lack of a distinct Internet voting authority. In response to this criticism, Estonia recently amended its election laws to create an electronic voting committee that would report to the National Electoral Committee.

France also made special provisions to accommodate e-voting in its 2012 parliamentary election. It set up a seven-member office of electronic voting, consisting of heads of various government information and security boards, as well as members of the Assembly of French Citizens Abroad. They have the power to invalidate the election results and oversee security (OSCE 2012c). Similar to Estonia, the French board also takes custody of the encryption keys.

Norway did not set up a strict formalized oversight board for its pilot project, although the use of various government departments to handle security and oversee different components required cross-government co-operation to handle the election.

Critics fear that if the individuals in charge of electoral oversight do not have sufficient technical understanding, an electronic voting system may be too dependent on the programmers, outside contractors or technical staff involved in implementing the system.

Creating a broader committee or board to assist with the oversight of electronic elections in Canada may help address concerns that may arise from the novelty and technological complexity of conducting an election partly by Internet and the increased concentration of responsibility that will likely accompany it.

A board or committee could work either as a subset of Elections Canada, ultimately advising the Chief Electoral Officer, or as a distinct entity with its own inherent authority under a revised *Canada Elections Act*. If it acts as an advisory board, its functions would probably be limited to providing advice. If it had its own inherent authority, it would be possible to assign many of the tasks such as holding cryptographic keys or authorizing a shutdown to the board.

The exact composition of a board will require further discussion. Potential candidates include members of the judiciary, heads of national security agencies who would be familiar with technical threats, as well as academics or industry professionals. The most important factors will be whether the public perceives the board as being independent and whether major stakeholders including political parties will have confidence in the appointment process.

Summary of Recommendations

The centralized and technical nature of e-voting requires effective and independent oversight. Public confidence in the system will be enhanced if those overseeing electronic voting have the technical expertise, independence, reliability and multiparty support to make tough decisions related to e-voting. Further discussion is required to determine whether this would be most effective within the electoral authority or with a new body with independent powers. We recommend that the electoral authority and those representing various political parties work together to create a board or committee with the authority to make recommendations to the electoral authority or arrive at certain determinations regarding e-voting oversight. Potential members include:

- federal court judges or others with positional independence
- tenured academics specializing in engineering, computer science or law
- privacy or information commissioners
- others recommended by various political parties

5.0 CONCLUSION

Any introduction of technology into the voting process is accompanied by a substantial number of risks, both known and unforeseeable, that have the potential to affect the results of an election. It is the responsibility of governments looking to implement electronic voting to take appropriate legislative measures to mitigate and prepare for factors that may affect the results of an election, as well as ensuring that the public can have confidence in the processes used.

The higher the level of risk, the more processes ought to be implemented to maintain the public's confidence in the electoral system and ensure that the effective right to vote is not displaced.

For our purposes, the notion of functional equivalence is useful during the comparative exercises in order to understand the sufficiency of procedures and ensure that adopting technology does not unnecessarily introduce new risks without corresponding benefits. Electronic options must be compared with the benefits and risks of their traditional equivalents, rather than against an abstract standard of perfection.

The legal framework for an e-voting test project or widespread usage can have a variety of formats. Standards, rules and other normative requirements may be contained in legislation, subordinate regulations or direction by Elections Canada contained in policy statements, manuals, requests for proposals from vendors and other contractual documents. As public confidence is always a crucial dimension of any voting system, we recommend that the electoral authority ensure that principles, standards and procedures are provided with reasonable transparency and clarity. The electoral authority should also take pains to ensure that innovations are explained to Canadians and that voters who actually use any new system are comfortable with using it and are not confused and misled.

Currently, the *Canada Elections Act* may be sufficient to authorize Internet voting in a test environment in a by-election or general election. Other jurisdictions have launched e-voting tests with minimal legislative changes. On the other hand, if some controversial decisions are made, such as those restricting voter participation in e-voting or reacting to a breakdown, there may be advantages to having Parliament legislate procedures and at least the minimal requirements. The stakes would be higher, and the potential for breakdown and tampering greater, if and when e-voting were to be used for a general election. Preferably, the *Canada Elections Act* would be amended to include at least the minimum standards, contingency plans and offences. The content of the legislation would, it is hoped, benefit from the deliberation and practical experience acquired through earlier pilot projects, as well as through looking at comparable jurisdictions and the principles of functional equivalence.

The ideal legal framework appears to be one that demands broad consultation and contemplates risks, problems and threats. It will require strong security measures and testing, but it also outlines clear steps to take if worst-case scenarios occur. It will offer clear legislative standards, but allow the electoral authority considerable flexibility to adopt the most advanced technology.

The legal framework for e-voting should deliver facilitated accessibility and reasonable accommodation, ensure voters are treated fairly and their choices remain secret, and guarantee accurate and prompt results. To do so, the framework should ensure there are comprehensible and transparent processes, a high level of risk assessment and security, adequate remedial contingencies, legislative certainty for all major electoral tasks and effective and independent oversight. This should be done in a way that can justify the costs and efficient use of resources.

Ultimately, whether we use paper or computers to vote, the goal should be to ensure as many Canadians vote as possible, while providing the public confidence that the voting system will perform as Canada's democratic tradition requires.

In conducting our research on what an ideal legal framework for Canada would be, we consulted with major reports on e-voting produced by government agencies as well as guidelines produced by international election observers. This is an overview of the key findings and criteria synthesized from those reports.

A.1 Council of Europe

The Council of Europe (COE) has released the only set of specific Internet voting standards that are valid and approved at an international level (Smith 2006). In 2004, the COE released the *Legal, Operational, and Technical Standards for E-voting* (Recommendation Rec (2004)11) (COE 2005), which was a guide to the legal, operational and technical standards for e-voting. Canada currently holds observer status to the COE. In addition to the recommendations, the COE has also released handbooks on implementing e-voting.

The COE's main recommendations comprise 121 requirements that serve as a checklist for implementing e-voting and that have been highly referenced by member nations, including Norway and Switzerland, in implementing their e-voting systems.

The COE framework itself is light on legal specifics, recognizing the wide range of national electoral legislation. Instead the focus is on specific best practices such as accessibility, security and practical elements of e-voting. The purpose is to encourage its member states to counter low voter turnout by embracing informational and communication technology used in day-to-day life. The council recommends that public confidence be built by ensuring that e-voting systems are "secure, reliable, efficient, technologically robust, open to independent verification and easily accessible to voters" (COE 2005, 7). To encourage this, the COE recommends that members change domestic legislation to meet the criteria, as well as ensure e-voting elections are as reliable and secure as those that do not use electronic means.

The recommendations are divided into three components: the legal, operational and technical steps that must be taken. The legal component embraces some general principles such as universal suffrage, equal suffrage and free suffrage, as well as the protection of election results. Many of the recommendations echo features that transcend voting methods, such as preventing a voter from voting multiple times, not disturbing freedom of choice and properly preparing registration lists.

Components of Council of Europe Recommendations
Legal Recommendations ■ Principles (universal suffrage, equal suffrage, free suffrage) ■ Procedural safeguards (transparency, verifiability and accountability, reliability and security) Operational Recommendations ■ Notifications, voting, results Technical Recommendations ■ Accessibility, interoperability (ability of various technical components to operate together), system operation, security, audits, certification
Recommendations include the following technical and design standards:
■ Make interfaces clear and useable (recommended standard number 1) ■ Ensure the systems' use is maximized by the disabled (standard number 3) ■ Keep e-voting as an additional and optional means of voting (standard number 4) ■ Ensure users can cast a blank ballot (standard number 13)

■ Allow voters to break off voting at any time (standard number 11) ■ Protect user privacy (various recommended standards)
Examples of specific procedural requirements are the following:
■ The public should be educated and be confident (recommended procedure number 20) ■ Information should be publicly available (procedure number 21) ■ Advance testing and trial by voters is recommended (procedure number 22) ■ Observers should be permitted to observe and comment on elections (procedure number 23) ■ Independent testing should be conducted before the system is used (procedure number 25) ■ Steps should be taken to prevent fraud or unauthorized intervention (procedure number 29) ■ All changes to the system should require teams of two (procedure numbers 32 and 33) ■ Remote voting should not end at a later time than poll stations (procedure number 45) ■ Steps should be taken to prevent linking voters with the votes (procedure number 48)

Much of the report is very specific, containing steps to ensure that privacy, security and systems are adequately tested; that proper audit methods are in place; and that backup plans are in place in case there are any hardware failures. It is now becoming common for election observers to use the COE's recommendations as a report card to test system requirements and procedures, and we would recommend that election officials in Canada consider referencing this checklist as well.

Not all of the recommendations are universally adopted. For instance, there is debate on whether a voter should be able to get a receipt for having voted, as some feel it can lead to voter coercion, while others feel that a paper trail of some sort may help voter confidence. Nor are the recommendations entirely complete. They do not address specific laws that should be in place to prevent election fraud or what is the best way to distribute tasks in an electronic voting system.

A2 United States Election Assistance Commission

The United States Election Assistance Commission has released comprehensive guidelines for the use of controlled e-voting systems, but has yet to release the same requirements for Internet voting. The commission was created in 2002 through the *Help America Vote Act of 2002*, a bill passed by the US Congress to encourage states to replace outdated punch card and lever-based voting systems that were controversial in the 2000 presidential election, particularly in some of the Florida counties. The *Help America Vote Act of 2002* legislates some minimum standards, while the National Institute of Standards and Technology advises the commission on a set of specific guidelines.

Voluntary Voting System Guidelines is a set of criteria governing the use of controlled voting machines that use direct-recording electronic technology.[12] While each US state independently administers federal and state elections, states that comply with the minimum requirements of the *Help America Vote Act of 2002* are eligible for federal funding toward the purchase of voting machines. Some states have adopted the Voluntary Voting System Guidelines certification requirements directly, while others have set their own guidelines.

[12] Direct-recording electronic machines are one common form of controlled voting technology, and the one most commonly associated with electronic voting in the United States.

Mandatory Minimum Requirements of the *Help America Vote Act of 2002*
■ Creation of an independent Election Assistance Commission ■ Requirement for one direct-recording electronic or assisted voting machine to be at each polling place ■ Requirements for a paper ballot ■ Ability for voters to verify their choice before voting ■ Stipulation that the Election Assistance Commission creates voluntary guidelines, but states are free to choose their own means
Topics Covered by the Voluntary Voting System Guidelines
Performance guidelines: ■ Functional requirements ■ Usability and accessibility (including colour, contrast, test size) ■ Hardware, software and telecommunications requirements ■ Quality assurance and configuration management Certification testing guidelines: ■ Functionality testing ■ Hardware and software testing ■ System integration and quality assurance

The *Help America Vote Act of 2002* also requires the Election Assistance Commission to conduct a study of Internet-based voting, but this appears to be a subset of other studies. We have found a general survey of Internet voting, but no detailed guidelines to the extent of the Voluntary Voting System Guidelines.

Some criticism has been levelled against the Voluntary Voting System Guidelines criteria, because once technology is certified, there was no requirement that recertification would have to happen, and the guidelines have been slow to adapt to new threats. Some states such as California have adopted additional requirements that any errors or problems that become known must be immediately reported on threat of substantial fines.

A.3 Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) is a European-based oversight group that, among other things, sends election observers to almost every major European election to provide a report card and review of election procedures. The OSCE's reports are excellent for providing independent information on how elections take place in practice. We used its reports on Norway, the Netherlands, Estonia and others to identify areas and deficiencies that other jurisdictions came across in running their e-voting elections.

The OSCE's *Election Observation Handbook* (OSCE 2010) instructs its observers to observe practices in how nations conduct their voting, which is useful for observers examining both paper balloting as well as Internet voting. The handbook notes that some of the following steps are the best way to ensure voter confidence in any electoral system.

Organization for Security and Co-operation in Europe Key Legal Requirements
■ Transparent certification of systems and reporting of results ■ Independent testing by academics or certification bodies ■ Regulations to avoid conflicts of interest with third parties

■ Strong auditing methods at defined times ■ Divided responsibility among officials, vendors and testers
Common Deficiencies and Problems with Legal Frameworks
■ Lack of an adequate legal framework ■ Lack of manual-audit capacity ■ Lack of access to the source code ■ Lack of public confidence in the integrity of electronic-voting equipment ■ Insufficient training of election officials ■ Lack of information provided to voters ■ Lack of transparency in the certification process ■ Lack of division of responsibility among vendors of equipment, certification agencies and election administration ■ Lack of clear guidance or regulations in cases of equipment failure

The OSCE's early reports strongly recommended paper ballots, but this was for stand-alone kiosks in a controlled environment where there was a concern with tampering of individual voting machines.

A.4 International Foundation for Electoral Systems

The International Foundation for Electoral Systems (IFES), a non-governmental organization, has long been an expert in reviewing elections law, on topics including proportional representation, voter fraud and e-voting. IFES consists of academics and other experts in legal affairs who routinely consult and work with developing nations to implement election laws. It has released excellent handbooks on conducting feasibility studies for e-voting elections, as well as implementing solutions. In its recent report, *International Experience with E-Voting* (Barrat i Esteve et. al, 2012b), the IFES presented a broad survey of many of the considerations that are needed for e-voting, which was invaluable for our research. The foundation conducted an in-depth study on the recent Norwegian pilot projects. In its 2011 report, *Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies* (Goldsmith 2011), the IFES highlighted the importance of reviewing existing legislation and recommending changes to accommodate voting technology.

International Foundation for Electoral Systems Key Recommendations for Legal Systems
■ Making changes to election laws to ensure observers can access all key components of the election administration process ■ Implementing security mechanisms and safeguards to ensure accuracy and integrity of elections ■ Putting in place requirements for initial and periodic certification of technology, including who can conduct it and what the consequences of failure would be ■ Having legal contingencies for failure of an auditing mechanism or deciding which record takes precedent if there are differing records ■ Specifying whether there are mandatory audits in place ■ Considering the mechanism in place for challenging results

A.5 The Carter Center

The Carter Center, a US-based charitable organization, among other things sends election observers to many developing nations and helps to build civil society in many countries. The center has worked with the United Nations on developing an international framework for election observers. Because most of the elections it covered are in jurisdictions with little cultural similarities to Canada or were involving voting machines, we did not use its cases studies in our report. However, *The Carter Center Handbook on Observing Electronic Voting* (The Carter Center 2012) provides a guide for observers on what they should look at when examining a legal framework. While the handbook is not aimed at Internet voting, we found the considerations very helpful in designing a comprehensive legal framework for e-voting.

Carter Center Legal Framework Key Considerations
1. How does the legal framework for e-voting protect fundamental human rights and support obligations for democratic elections (including whether secrecy is protected)? 2. Is the legal framework clear and consistent regarding the use of e-voting technologies? (Is it in legislation or ad hoc?) 3. Who are the key stakeholders related to the use of e-voting in this electoral process? What are their respective roles according to the law? (For example, is there a technical subcommittee or an independent technological advisory body?) 4. Does the law allow independent, third-party inspection of the system and observation by domestic and international observers and candidates, parties and their agents? 5. Does the law require a voter-verified paper audit trail, and what is the legal relationship of this record to other records of the vote? 6. Does the electoral calendar allow enough time for all aspects of the process? 7. What tests or certification of the system is legally required? 8. What are the election day procedures as outlined in law? 9. What security and contingency plans are prescribed by law? (Do the electoral offences cover e-voting?) 10. What provisions are in place for the resolution of electoral disputes regarding the use of e-voting technologies? 11. Are there major gaps or flaws in the legal framework regarding the use of e-voting?

Additionally, The Carter Center raised other issues about what steps are taken to inform the voters and increase their confidence. Was the technology tendering process open? Who has ownership to the intellectual property? Is there a contingency plan in place for technology failure?

A.6 Canadian Research

For the purpose of our recommendations, we think is it important to also recognize some of the considerations that have begun to surface in other discussion papers regarding e-voting.

A discussion paper produced by Elections BC, the electoral authority in the province of British Columbia, identified seven criteria for e-voting (Elections BC 2011).

Elections BC Discussion Paper Criteria for E-voting
1. Accessibility: This includes recommendations such as maintaining a user-friendly interface, promoting public access and not using the Internet as the sole means of voting. 2. Equal voting power: This includes recommendations about centralizing lists of who has voted, as well having in place methods to allow multiple votes but only to maintain the last one. 3. Secrecy: This includes recommendations on using cryptographic processes as well as allowing voters to vote multiple times to reduce voter coercion. 4. Security: This consists of recommendations on identifying threats and designing technology to combat these threats. 5. Auditability: This consists of recommendations to ensure that voters are able to verify that their votes were counted as they intended to. Additionally, this also refers to the ways in which the system and hardware are tested, certified and relied upon by experts. 6. Transparency and simplicity: This includes recommendations that mainly involve ensuring that transparency, openness and simplicity are kept in mind and that as much of the testing, auditing procedures and implementation plans are available for public review.

Like some of the other sources, many of the considerations in the Elections BC report span both the legal and technical requirements.

B.1 Literature

Allen Consulting Group. 2011. "Evaluation of Technology Assisted Voting Provided at the New South Wales State General Election March 2011." Melbourne, Australia: Allen Consulting Group. www.elections.nsw.gov.au/__data/assets/pdf_file/0004/93766/July_2011_Final_ACG_iVote_Report_ELE01-C_Final.pdf

Alvarez, Michael R., and Thad E. Hall. 2008. *Electronic Elections: The Perils and Promises of Digital Democracy.* Princeton, NJ: Princeton University Press.

Alvarez, Michael, Gabriel Katz and Julia Pomares. 2011. "The Impact of New Technologies on Voter Confidence in Latin America: Evidence from E-voting Experiments in Argentina and Colombia." *Journal of Information Technology & Politics* 8, 2: 199–217.

Australian Electoral Commission. 2008. "Evaluation of the Remote Electronic Voting Trial for Overseas Based ADF Personnel Electors at the 2007 Federal Election." www.aec.gov.au/voting/files/adf_final_evaluation.pdf

Barrat i Esteve, Jordi, Ben Goldsmith and John Turner. 2012a. "Speed and Efficiency of the Vote Counting Process – Norwegian E-Vote Project." Washington, DC: International Foundation for Electoral Systems. www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic4_Assessment.pdf

———. 2012b. "International Experience with E-voting – Norwegian E-Vote Project." Washington, DC: International Foundation for Electoral Systems. www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf

———. 2012c. "Compliance with International Standards – Norwegian E-Vote Project." Washington, DC: International Foundation for Electoral Systems. www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

Beaucamps, Phillippe, Daniel Reynaud-Plantey, Jean-Yves Marion and Eric Filiol. 2009. "On the Use of Internet Voting on Compromised Computers," *ICIW '09: Proceedings of the 4th International Conference on Information Warfare and Security*.

Boyer, Patrick. 1981. *Political Rights: The Legal Framework of Elections in Canada.* Toronto, Ont: Butterworths.

Brightwell, Ian. 2011. "iVote Technology Assisted Voting: NSW State Election 26 March 2011." Sydney, Australia: New South Wales Electoral Commission. www.elections.nsw.gov.au/__data/assets/pdf_file/0007/94246/IE_Aust_Presentation_25_August_2011_v8.pdf

Buckland, Richard, and Roland Wen. 2012. "The Future of E-voting in Australia." *IEEE Security & Privacy* 10, 5: 25–32. DOI 10.1109/MSP.2012.59.

Canada–Europe Transatlantic Dialogue. 2010. "Internet Voting: What Can Canada Learn? Internet Voting Workshop Summary of Proceedings." Policy Workshop, January 26. www.canada-europe-

dialogue.ca/events/2010-01-26-InternetVotingMaterials/2010-01-26-(E)Workshop_Proceedings_FINAL(April19).pdf

The Carter Center. 2012. *The Carter Center Handbook on Observing Electronic Voting*. Atlanta, GA: The Carter Center. www.cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf

Castellani, Luca. 2010. "UNCITRAL Legislative Standards on Electronic Communications and Electronic Signatures: An Introduction." www.itu.int/dms_pub/itu-t/oth/15/08/T15080000020001PDFE.pdf

Chevallier, M., W. Warynski and A. Sandoz. 2006. "Success Factors of Geneva's e-voting System." *The Electronic Journal of e-Government*, 4, 2: 55–62.

Commission on Electronic Voting. 2007. "Second Report of the Commission on Electronic Voting: Secrecy, Accuracy and Testing of the Chosen Electronic Voting System." Dublin, Ireland: Commission on Electronic Voting. www.umic.pt/images/stories/publicacoes1/Part%200%20Index.pdf

Council of Europe (COE). 2005. *Legal, Operational, and Technical Standards for E-voting* (Recommendation Rec(2004)11). Strasbourg, France: Council of Europe Publishing. www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

———. 2010a. *E-voting Handbook*. Strasbourg, France: Council of Europe Publishing. www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf

———. 2010b. "Third Meeting to Review Developments in the Field of E-voting Since the Adoption of Recommendation Rec(2004)11 on Legal, Operational and Technical Standards for E-voting." Strasbourg, France: Council of Europe. www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/GGIS(2010)19%20E%20corr.%20Meeting%20Report%20e-voting%20review%202010%2021%2012%2010.asp

Delvinia Interactive Inc. 2004. *Internet Voting and Canadian e-Democracy in Practice: The Delvinia Report on Internet Voting in the 2003 Town of Markham Municipal Election*. Toronto, Ont.: Delvinia Interactive Inc. www.delvinia.com/egov/Delvinia_Voting_Report_04.pdf

Elections BC. 2011. "Discussion Paper: Internet Voting." Victoria, BC: Elections BC.

Elections Canada. 2011a. "Report of the Chief Electoral Officer of Canada – Following the Pilot Project on the Use of an Assistive Voting Device in the November 29, 2010, By-election held in Winnipeg North." Ottawa, Ont.: Elections Canada.

———. 2011b. "Report of the Chief Electoral Officer of Canada on the 41st General Election of May 2, 2011." Ottawa, Ont.: Elections Canada.

Elections Quebec. 2006. "Evaluation Report of New Methods of Voting - The Chief Electoral Officer Makes a Disturbing Diagnosis of the Problems that Occurred during the Municipal Elections of November 6, 2005." Québec, Que.: Elections Quebec. www.electionsquebec.qc.ca/english/news-detail.php?id=2146.

The Electoral Commission. 2007a. “Electronic Voting: May 2007 Electoral Pilot Schemes.” London, UK: The Electoral Commission. www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0008/13220/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf

———. 2007b. “Key Issues and Conclusions: May 2007 Electoral Pilot Schemes.” London, UK: The Electoral Commission. www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/Keyfindingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf

Electronic Frontier Finland. 2009. *A Report on the Finnish E-voting Pilot.* Finland: Electronic Frontier Finland. www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf

E-Mergent Management Research. 2010. “A Study of Internet Voting Security Risks and Accessibility Opportunities for the Town of Markham.” Markham, Ont.: Town of Markham.

Estonian National Electoral Committee. 2004. “Kasutusloomudeli ülevaade, document EH-04-02-01.” Tallinn, Estonia: Estonian National Electoral Committee. www.vvk.ee/public/dok/Kasutusloomudeli-ylevaade-EH-04-02-01.pdf

———. n.d. “Statistics about Internet Voting in Estonia.” www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

Funke, Alice. n.d. “2011 General Election.” Pundits’ Guide to Canadian Federal Elections. www.punditsguide.ca/elections/?elec_event=26&qry=8

Geist, Michael. 2010 (March 9). “Casting a Vote Against Internet Voting.” www.michaelgeist.ca/content/view/4849/159/

———. 2012 (March 31). “Internet Voting Carries Risk as Shown by NDP Experience.” *Toronto Star*.

Goldsmith, Ben. 2011. *Electronic Voting & Counting Technologies: A Guide to Conducting Feasibility Studies.* Washington, DC: International Foundation for Electoral Systems. www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf

Gonggrijp, Rop et al. 2006. “Nedap/Groenendaal ES3B Voting Computer: A Security Analysis.” The Netherlands: The “We Do Not Trust Voting Computers” Foundation. http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

Goodman, Nicole, Jon Pammet and Joan DeBardeleben. 2010. “A Comparative Assessment of Electronic Voting.” Ottawa, Ont.: Elections Canada. www.elections.ca/res/rec/tech/ivote/comp/ivote_e.pdf

Government of Canada. 2012. “GC Information Technology Incident Management Plan.” Ottawa, Ont.: Treasury Board of Canada Secretariat. www.tbs-sct.gc.ca/sim-gsi/sc-cs/docs/itimp-pgimti/itimp-pgimti01-eng.asp

Hall, Joseph Lorenzo. 2006. “Transparency and Access to Source Code in Electronic Voting.” USENIX/ACCURATE Electronic Voting Technology (EVT'06) Workshop. http://josephhall.org/papers/jhall_evt06.pdf

Heiberg, Sven, Peeter Laud and Jan Willemson. 2011. “The Application of I-voting for Estonian Parliamentary Elections of 2011.” http://research.cyber.ee/~jan/publ/evote2011.pdf

Hogg, Peter. 2007. *Constitutional Law of Canada*, 5th edition. Toronto, Ont.: Carswell.

Hole, Kjrell, and Lars-Hell Neglen. 2010. "Towards Risk Assessment of Large-Impact and Rare Events." *IEEE Security & Privacy*, 8, 3: 21–27.

Jones, Douglas, and Barbara Simons. 2012. *Broken Ballots: Will Your Vote Count?* Stanford: CLSI Press.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. Toronto, Ont.: Doubleday Canada.

Kapoor, K. C. 2011. "Online Voting System. eGov: Best Urban ICT Initiative of the Year." http://awards.eletsonline.com/2011/11/15/online-voting-system.

Karhumäki, Juhani, and Tommi Meskanen. 2008. "Audit Report on Pilot Electronic Voting in Municipal Elections." Turku, Finland. www.vaalit.fi/uploads/5bq7gb9t01z.pdf

Kelly, Sanja, and Sarah Cook (eds.). 2011. *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*. Washington, DC: Freedom House. www.freedomhouse.org/sites/default/files/FOTN2011.pdf.

Kumar, Sanjay. 2011. "Analysis of Electronic Voting System [sic] in Various Countries." *International Journal on Computer Science and Engineering* 3, 5: 1825–30.

Lundell, Jonathan. 2007. "Review: Irish Commission on Electronic Voting." *Voting Matters* (McDougall Trust), Issue 23: 13–17.

Martens, Tarvi. 2010. "Internet Voting in Estonia." http://canada-europe-dialogue.ca/events/2010-01-26-InternetVotingMaterials/TarviMartens.pdf

———. 2012. Interview on June 20, 2012.

Melia, Paul, and Luke Byrne. 2012 (June 29). "€54m Voting Machines Scrapped for €9 Each." *Irish Independent*. www.independent.ie/national-news/54m-voting-machines-scrapped-for-9-each-3153437.html

New South Wales Electoral Commission. 2011. "iVote: Technology Assisted Voting Approved Procedures for NSW State General Election 2011." Sydney, Australia: New South Wales Electoral Commission. www.elections.nsw.gov.au/publications/policies/ivote_approved_procedures

Norwegian Ministry of Local Government and Regional Development. 2006. "Electronic Voting: Challenges and Opportunities." www.regjeringen.no/upload/kilde/krd/red/2006/0087/ddd/pdfv/298587-evalg_rapport_engelsk201106.pdf

———. 2009. "E-vote 2011: System Requirements Specification." www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf

———. 2011. "Project Mandate for E-vote 2011 Project." www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Prosjektdirektiv_evalg2011_English.pdf

Open Rights Group. 2007. "May 2007 Election Report: Findings of the Open Rights Group Election Observation Mission in Scotland and England." London, UK: Open Rights Group. www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf

Organization for Security and Co-operation in Europe (OSCE). 2006. “Netherlands. Parliamentary Elections, 22 November 2006. Election Assessment Mission Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/elections/netherlands/24322

———. 2007. “Republic of Estonia Parliamentary Elections, 4 March 2007. Election Assessment Mission Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/elections/estonia/25925

———. 2010. *Election Observation Handbook*, Sixth edition. Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/elections/68439

———. 2011. “Estonia Parliamentary Elections, 6 March 2011. Election Assessment Mission Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/77557

———. 2012a. Switzerland. “Swiss Confederation Federal Assembly Elections, 23 October 2011. Election Assessment Mission Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/87417

———. 2012b. “Norway: Internet Voting Pilot Project: Local Government Elections, Election Expert Team Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/88577

———. 2012c. “Republic of France Parliamentary Elections 10 and 17 June, 2012. Needs Assessment Mission Report.” Warsaw, Poland: Organization for Security and Co-operation in Europe. www.osce.org/odihr/elections/90763

Organization of American States (OAS). 2001. *Inter-American Democratic Charter*. Washington, DC: Organization of American States. www.oas.org/OASpage/eng/Documents/Democractic_Charter.htm

Paris, Maeve. 2004. “Accessible Democracy and Electronic Voting in the Republic of Ireland.” *Information Technology and Disabilities* 10, 2.

Pieters, Wolter, and M. J. Becker. 2005. “Ethics of E-voting: An essay on Requirements and Values in Internet Elections.” *Ethics of New Information Technology: Proceedings of the Sixth International Conference of Computer Ethics* (CEPE2005), 17–19 Jul 2005, Enschede, The Netherlands; 307–318. Centre for Telematics and Information Technology, University of Twente. http://eprints.eemcs.utwente.nl/13894/.

PricewaterhouseCoopers. 2011. “Technology Assisted Voting Audit: Post Implementation Report.” Sydney, Australia: PricewaterhouseCoopers. www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf

Prolexic. 2012. “Prolexic Attack Report: Q1 2012.” Hollywood, FL: Prolexic. www.prolexic.com/pdf/ProlexicQ12012AttackReport.pdf.

République et Canton de Genève. 2009. “Online Voting: Challenges and Outcomes.” www.geneve.ch/evoting/english/presentation_projet.asp

Rubin, Avi. 2007 (August 26). “The Virus Did It.” http://avi-rubin.blogspot.ca/2007/08/virus-did-it.html.

Ruus, Kertu. 2008. “Cyber War I: Estonia Attacked from Russia.” *European Affairs* (European Institute), 9, 1-2. www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html.

Scytl. 2012. “French Expats Vote Online in Legislative Elections with Scytl’s Technology.” Company news release, July 11. Barcelona, Spain: Scytl. http://eon.businesswire.com/news/eon/20120711005780/en/Scytl/France/Ministry-of-Foreign-Affairs

Scytl Canada. 2012. “NDP Leadership Vote Result Not Compromised by ‘Malicious, Orchestrated Effort’ to Clog Online Balloting System at Weekend Convention, Says Scytl Canada.” Company news release, March 27. Toronto, Ont.: Scytl Canada. www.newswire.ca/en/story/944715/ndp-leadership-vote-result-not-compromised-by-malicious-orchestrated-effort-to-clog-online-balloting-system-at-weekend-convention-says-scytl-canada

Shaffer, Frederick Charles. 2008. “Clean Election Reform and Its Hidden Costs: Lessons from Florida and Quebec.” www.wcfia.harvard.edu/sites/default/files/Clean%20Election%20Reform%20And%20Its%20Hidden%20Costs%20Schaffer.pdf

Smith, Justice Matthew. 2006. “Second Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System.” Dublin, Ireland: Commission on Electronic Voting. www.umic.pt/images/stories/publicacoes1/Part%200%20Index.pdf

United Nations. 1999. “UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.” New York, NY: United Nations Publications. www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

United States Election Assistance Commission (US EAC). 2005. *Voluntary Voting System Guidelines*. Washington, DC: US Election Assistance Commission. www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx

———. 2011. “A Survey of Internet Voting.” Washington, DC: US Election Assistance Commission. www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

Volkamer, Melanie, Oliver Spycher and Eric Dubuis. 2011. “Measures to Establish Trust in Internet Voting.” ICEGOV 2011, Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, September 26–28, 2011, Tallinn, Estonia.

Wolchok, Scott, Eric Wustrow, Dawn Isabel and J. Alex Halderman. 2012. “Attacking the Washington, D.C. Internet Voting System.” Proc. 16th Conference on Financial Cryptography & Data Security, February 2012.

Young, John Hardin, ed. 2009. *International Election Principles: Democracy and the Rule of Law*. Chicago, IL: American Bar Association.

B.2 Case Law

Cusimano v. Toronto (City), 2011 ONSC 2527
Dixon v. British Columbia (Attorney General), 59 DLR (4th) 247; [1989] 4 WWR 393; 35 BCLR (2d) 273
Figueroa v. Canada (Attorney General), 2003 SCC 37

Haig v. Canada (Chief Electoral Officer), [1993] 2 SCR 995
Henry v. Canada (Attorney General), 2010 BCSC 610
Hoogbruin v. A.G.B.C., 24 DLR (4th) 718; [1986] 2 WWR 700; 20 CRR 1; 70 BCLR 1
Hughes, James Peter v. Election [sic] *Canada*, 2010 CHRT 4
Opitz v. Wrzesnewskyj, 2012 SCC 55
Re Ontario Film and Video Appreciation Society, (1984) 45 OR (2d) 80
Reference re Prov. Electoral Boundaries (Sask.), [1991] 2 SCR 158
Wrzesnewskyj v. Attorney General (Canada). 2012 ONSC 2873

Australia, *Yarran v. Blurton*, [1992] FCA 260 (Federal Court of Australia, June 1992)
Estonia, *Constitutional Judgement 3-4-1-13-05* (Constitutional Review Chamber of the Supreme Court, September 2005)
Finland, *KHO:2009:39* (Supreme Administrative Court, April 2009)
Germany, *BVerfG*, *2 BvC 3/07* (Federal Constitutional Court, March 2009)
United States, *Voting Integrity Project v. Fleisher,* 4 ILRD 549 (Arizona District Court, March 2000)

B.3 Legislation and Regulations

Canadian

Access to Information Act, RSC 1985, c A-1
Canada Elections Act, SC 2000, c 9
Canadian Human Rights Act, RSC, 1985, c H-6
The Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11 [Charter]
Personal Information Protection and Electronic Documents Act, SC 2000, c 5
Secure Electronic Signature Regulations (SOR/2005-30)

Alberta: *Election Act,* RSA 2000, c E-1
Nova Scotia: *Municipal Elections Act,* RSNS 1989, c 300
Ontario: *Electronic Commerce Act*, 2000, SO 2000, c 17
Ontario: *Municipal Elections Act*, 1996, SO 1996, c 32, Sch
Quebec: *An Act to Establish a Legal Framework for Information Technology*, RSQ, c C-1.1

International

California, *California Elections Code*
Estonia, (*Parliament) Election Act*, 2002
Estonia, *Penal Code*, RT I 2001, 61, 364
France, *Electoral Code*, article R176-3-2
Gujarat (India), *Urban Development and Urban Housing Department Orders* (June 5, 2010)
New South Wales, *Parliamentary Electorates and Elections Act 1912* No 41
Norway, *Pilot Schemes in Public Administration Act* (Act No. 87 of 26 June 1992)
Norway, *Representation of the People Act* (Act No. 57 of 28 June 2002) Regulations relating to trial electronic voting. FOR 2011-03-31
Switzerland, *Federal Act on Political Rights*. *SR 161.1*, Title 1
United Nations, *International Covenant on Civil and Political Rights,* 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171
United States, *Help America Vote Act of 2002* (Pub. L. 107–252)