

Electronic Thesis and Dissertation Repository

6-7-2024 11:45 AM

Cyber Risks in Ontario Online Elections

James D. Brunet, *Western University*

Supervisor: Essex, Aleksander, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Electrical and Computer Engineering

© James D. Brunet 2024

Follow this and additional works at: <https://ir.lib.uwo.ca/etd>



Part of the [Digital Communications and Networking Commons](#)

Recommended Citation

Brunet, James D., "Cyber Risks in Ontario Online Elections" (2024). *Electronic Thesis and Dissertation Repository*. 10185.

<https://ir.lib.uwo.ca/etd/10185>

This Dissertation/Thesis is brought to you for free and open access by Scholarship@Western. It has been accepted for inclusion in Electronic Thesis and Dissertation Repository by an authorized administrator of Scholarship@Western. For more information, please contact wlsadmin@uwo.ca.

Abstract

Online voting is increasingly prevalent in Ontario's municipalities, despite a lack of regulated technological and procedural safeguards. Individual municipalities, lacking deep knowledge of online voting technologies, are responsible for procuring technology from private vendors which make security and privacy claims that are difficult to verify. These reasons, among others, have contributed to an anomalous environment where election technology, security, and procedures diverge greatly from other robust democracies that use electronic voting. This thesis demonstrates this divergence by first presenting a novel security vulnerability in a popular online voting system used in Ontario, as well as the difficulty communicating this risk to other vendors active in the province. Then, through a broad standards-based review of online voting systems in Ontario, this thesis demonstrates that online voting systems, legislation, and municipal procedures fail to meet most of the Council of Europe's directives for online voting.

Keywords: Online voting - Standards - Cybersecurity - Ballot Secrecy - TLS - Privacy

Summary for Lay Audience

In Canada, in most elections, voters are required to vote on a piece of paper, which is then mailed or physically dropped in a ballot box. In federal elections, these paper ballots are counted by hand by election officials (with observers present to ensure the counting is fair).

Online voting, or electronic voting, is a relatively new practice of voting in elections by using a computer or mobile phone. Since 2003, online voting has become more popular specifically for elections at the municipal (city, town, county, etc.) level in Ontario. Online voting elections are very different from paper elections. One key difference is that votes can be counted by computer systems in a way that can be difficult to verify by independent observers.

There are potential risks at many stages of the online voting process: Computer systems that count votes could be tampered with, voters could be intimidated into voting a particular way, voters could be impersonated, the secrecy of the vote of voters could be compromised, etc. Despite these potential risks, not much research has been done into how these elections are conducted in Ontario, as well as how well municipalities in Ontario are doing in addressing these risks.

This thesis explores cyber risks to online voting in Ontario and finds that many risks have not been meaningfully addressed by municipalities and/or the companies that sell municipalities online voting systems. It contains two studies, the first of which is about the discovery of a major security vulnerability in an online voting solution used by dozens of municipalities. The first study also highlights the difficulty of reporting these vulnerabilities to companies that sell these online voting systems to municipalities. The second study compares practices in Ontario to Europe, by using international standards for online voting used in Europe as a benchmark. This study finds Ontario broadly fails to meet these European standards for accountable, reliable, secure, and transparent conduct for online elections.

These studies together make a strong argument that much work needs to be done to improve online elections in Ontario.

Acknowledgements

Thanks to Simply Voting, Swiss Post, and Neuvote for providing demo access. Thanks also to Jeremy Clark, Alex Halderman, Matthew Heuman, Brian Lack, Nicole Goodman, Iuliia Spycher Krivonosova, Michelle Blom, Philip Stark, and the anonymous reviewers for their valuable feedback.

Last, but certainly not least, thanks to Jana Baig for helping me stay focused and providing me with much-needed support in my time of need.

This work was supported by the National Science and Engineering Research Council of Canada's Discovery Grant program.

Co-Authorship Statement

The following thesis contains material from two conference papers that have been published and presented, both of which are primarily the works of James Brunet. These two papers are used as the main body of the thesis and were authored by James Brunet under the supervision of Dr. Aleksander Essex, and co-authored by James Brunet, Dr. Aleksander Essex, and Dr. Demetri Pananos.

Details of Collaboration With Co-authors

First Study: Discovery, Analysis and Mitigation of a Ballot Secrecy Vulnerability in a Real-World Election System

Paper: Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections

Status: Published and presented at the Seventh International Joint Conference on Electronic Voting, E-VOTE-ID 2022, Springer Nature Switzerland, Cham, 2022, pp. 36–52.

Estimated Contribution of Student: 70% of the combined manuscript and research work.

James Brunet: Responsible for nearly all research work. Evaluated and analyzed production e-voting systems to determine their configuration and see if vulnerabilities existed, developed a duplicate of the production e-voting system with limited functionality using Flask, deployed this duplicate system including configuring Apache, DNS and TLS, developed and ran a script to simulate and monitor encrypted traffic between voters and the e-voting system, collected data on TLS record lengths, performed preliminary data analysis. Led presentation of vulnerability to Simply Voting as part of coordinated disclosure.

Also responsible for a plurality of the manuscript work. Wrote the description of Simply Voting’s system, methodology section, information about data collection for both experiments, subsection about candidate combination subsets in Experiment 3, and most of the mitigations section. Edited all sections.

Demetri Pananos: Performed in-depth data analysis for all experiments, wrote Data Analysis section for Experiment 1, created confusion matrix.

Aleksander Essex: Communicated with e-voting vendors to arrange for demo access and share findings, wrote much of the introduction and related work. Contributed substantially to the conclusion and mitigations section. Edited all sections.

Second Study: A Standards-Based Review of Online Voting in Ontario Municipalities

Paper: Online Voting in Ontario Municipalities: A Standards-Based Review

Status: Published and presented at the Eighth International Joint Conference on Electronic Voting, E-VOTE-ID 2023, Springer Nature Switzerland, Cham, 2023, pp. 52–68.

Estimated Contribution of Student: 80% of the combined manuscript and research work.

James Brunet: Responsible for nearly all research work. Analyzed the Swiss Ordinance for Electronic Voting and the Council of Europe Standards for E-Voting. Searched for and analyzed public-facing election documents, election-related news articles, social media posts, statements from vendors and municipalities, minutes from municipal council meetings, as well as contracts and procurement documents for e-voting systems. Performed a passive security analysis of each of the five online voting vendors active in Ontario and performed a more thorough evaluation of demonstration systems offered by two vendors. Compared these evaluations to the Council of Europe Standards for E-Voting to evaluate whether directives were met, partially met, or unmet.

Also responsible for the majority of the manuscript work. Wrote details about data collection and described compliance categories. Wrote summary of findings section as well as analysis of selected directives, and created all tables in the study. Edited all sections.

Aleksander Essex: Provided advice and guidance on compliance categories for different directives. Wrote recommendations, most of the introductory remarks, as well as the terminology section. Edited all sections.

Contents

Abstract	ii
Summary for Lay Audience	iii
Acknowledgements	iv
Co-Authorship Statement	v
List of Figures	xi
List of Tables	xii
List of Appendices	xiii
List of Abbreviations, Symbols, and Nomenclature	xiv
1 Introduction	1
1.1 Background	1
1.1.1 No Standards for Online Voting in Ontario Municipalities	2
1.2 Problem Statement and Thesis Outline	2
1.3 Thesis Contribution	3
1.4 Thesis Statement	4
2 Related Work	6
2.1 Online Voting in Ontario	6
2.2 Principles of the Municipal Elections Act (MEA)	6
2.3 Verifiability	7
2.3.1 Definition	7
Individual Verifiability	8
Universal Verifiability	8
Eligibility Verifiability	8
2.3.2 Additional Requirements	9
Ballot Secrecy	9
Coercion Resistance	10
2.3.3 Proposed and Implemented Verifiable Voting Systems	11
2.4 Types of Threats to Online Voting	11
2.4.1 Attackers	12

2.4.2	Technical Infrastructure for Online Voting	12
	Voting Client & Voter Device	12
	Administrator Client & Administrator Device	13
	Voting Server	13
	Network Path	14
	DDOS Protection Providers	14
	Third-Party Software	14
2.5	Illustrative Examples of Online Voting Threats Relevant to Ontario	15
2.5.1	Flawed Verifiability	15
2.5.2	Insufficient Evidence	16
2.5.3	Weak Authentication Credentials	16
2.5.4	Client-side Vote-altering Malware	17
2.5.5	Client-side Count-altering Malware	17
2.5.6	Unauthorized Access to Voting Server	17
2.5.7	Online Voting Website Outage	18
2.6	Online Voting in Other Jurisdictions	18
2.6.1	Regulatory Safeguards	18
	Council of Europe’s Standards of E-Voting (SeV)	18
	Swiss Federal Chancellery Ordinance on Electronic Voting (OEV)	19
3	First Study: Secrecy Vulnerability in Real-World Election System	20
3.1	Introductory Remarks	20
3.2	Background and Related Work	21
3.3	Research Question and Scope	22
3.3.1	Vendor Demo Access Requests	22
3.4	Description of Simply Voting’s System	23
3.4.1	Ballot Casting Process	23
3.4.2	Potential Side-channel Attacks in the Ballot Casting Process	24
3.5	Methodology	24
3.5.1	Testing a Length-Based Side-channel Attack	25
3.5.2	Technical Implementation of the Client Application	25
3.5.3	Technical Implementation of the Server Application	26
	Observing Simply Voting’s Server Stack.	26
	Approximating Simply Voting’s Server Stack.	27
	Replicating Simply Voting’s Web Application.	28
3.6	Experiment 1 (Single contest): Township of Selwyn, Ward Lakefield	29
3.6.1	Data Collection	29
3.6.2	Data Analysis	30
3.7	Additional Experiments	31
3.7.1	Experiment 2 (Two contests): Township of Selwyn, Ward Ennismore	31
3.7.2	Experiment 3 (Three contests): Town of Ajax, Ward 1	32
3.8	Mitigations	33
3.8.1	Client-Side Confirmation Page Generation	33
3.8.2	Fixed-Length Responses	34
3.8.3	Uniformly Random-Length Padding in Response Header	34

3.8.4	Padding From a Gaussian Distribution	36
3.8.5	Discussion and Conclusion	36
4	Second Study: Standards-based Review of E-Voting in ON Municipalities	37
4.1	Introductory Remarks	37
4.2	Background and Preliminaries	38
4.2.1	Terminology	38
4.2.2	Information Collection About Ontario Municipal Online Voting Practices	39
4.2.3	Related Work	39
4.2.4	Compliance Categories	40
4.3	Summary of Findings	41
4.4	Analysis of Selected Directives	41
4.4.1	Directive Broadly Met	42
4.4.2	Directive Fully Met by Some Cities	43
4.4.3	Directive Partially Met by Most or All Cities	45
4.4.4	Directive Unmet: Meaningful Attempts From Some Cities	45
4.4.5	Directive Unmet by Almost All Cities	46
4.4.6	Directive Unmet by All Cities	47
4.4.7	Directive Unmet Due to Failure Within Provincial Jurisdiction	49
4.4.8	Not Applicable	49
4.4.9	Information Not Available	50
	Directives Requiring Access to ‘Live’ Election Systems	50
	Directives Requiring Knowledge of Vendor Procedures	50
	Directives Requiring Knowledge of Online Voting System Internals	50
	Directives Requiring Knowledge of Municipal Procedures	50
4.5	Recommendations and Conclusion	51
	Recommendation 1. Cities should be familiar with international demo- cratic principles, expectations and norms.	51
	Recommendation 2. Cities should conduct their own internal review.	51
	Recommendation 3. Province should update the Municipal Elections Act.	51
	Recommendation 4. Make information about e-voting policies, proce- dures and protections more widely available.	51
	Recommendation 5. Make election results evidence-based.	51
4.6	Summary of Analysis	53
5	Discussion, Future Work, and Conclusion	55
5.1	Discussion	55
5.1.1	Central Role of Private Sector	55
5.1.2	Implications of Vulnerabilities	55
5.1.3	Challenges in Mitigation	56
5.2	Future Work	56
5.2.1	Domestic Standards Development	56
5.2.2	Research in the 2026 Municipal Election	57
5.2.3	Public Access and Testing	57

5.2.4	Alternatives to PIN and Date of Birth Authentication	57
5.2.5	National Public Certification and Ownership	58
5.3	Conclusion	58
Bibliography		60
A Council of Europe Standards and Implementation Guidelines for E-Voting		66
Curriculum Vitae		76

List of Figures

3.1	Confusion Matrix (Proportions), Experiment 1. Rows normalized to sum to 1. Diagonal entries indicate class candidate-specific accuracy, while the other cells indicate proportion of votes for row candidate predicted to be the column candidate. As an example, 86% of votes for Black were correctly predicted to be for Black. 13% of votes for Black were predicted to be for Mitchell. The remaining 1% of votes for Black were predicted to be for Eales.	31
-----	---	----

List of Tables

2.1	Election Principles	7
3.1	Vendor responses to our demo request and associated findings.	23
3.2	Confirmation page DOM elements with varying values	24
3.3	2018 Municipal Ballot Options in Ward Ennismore, Township of Selwyn	26
3.4	Observed TLS Record Lengths (2,000 trials per candidate)	29
3.5	Performance on Test Set by Office, Experiment 2.	32
3.6	Proportion of Ballots by Possible Candidate Combinations, Experiment 2 (Cumulative).	33
3.7	Performance on Test Set by Office, Experiment 3.	33
4.1	Summary of compliance	41

List of Appendices

Appendix A Council of Europe Standards and Implementation Guidelines for E-Voting . 66

List of Abbreviations, Symbols, and Nomenclature

Abbreviations

API	Application Programming Interface
BREACH	Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext
CoE SeV	Council of Europe Standards of E-Voting
COVID-19	Coronavirus disease 2019
CRIME	Compression Ratio Info-leak Made Easy
CSIS	Canadian Security Intelligence Service
CSRF	Cross-Site Request Forgery
DC	District of Columbia
DGSI	Digital Governance Standards Institute
DOM	Document Object Model
E-Voting	Electronic Voting (AKA Online Voting)
E2E-V	End-to-End Election Verifiability
EMB	Election Management Body
gzip	GNU zip
HTML	Hypertext Markup Language
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
ISP	Internet Service Provider
JSON	JavaScript Object Notation
MEA	Municipal Elections Act
MIME	Multipurpose Internet Mail Extensions
MITM	Machine-in-the-Middle
OEV	Swiss Ordinance on Electronic Voting
OS	Operating System
PIN	Personal Identification Number

QR Code	Quick-Response Code
RCMP	Royal Canadian Mounted Police
RLA	Risk-Limiting Audit
SAFE Vote	Scratch Auditing for Fair Elections Vote
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UCP	United Conservative Party of Alberta
UI	User Interface
URL	Uniform Resource Locator
US VVSG	United States Voluntary Voting System Guidelines
VPS	Virtual Private Server
WCAG	Web Content Accessibility Guidelines

Symbols

π	Probability
θ	Unknown parameter of interest
B	The byte length of an encrypted vote V
C	A choice available to a voter for a particular office
k	A candidate for a particular office
o	Total number of offices on a ballot
T	The set of all possible candidate combinations that could be submitted by a voter
V	An encrypted vote

Glossary

Online voting	Also referred to as e-voting, online voting is a method of voting that allows voters to vote using an app or a web browser. Often, voters can vote at home, from their personal devices.
---------------	--

Malware	Malicious software that is designed to gain unauthorized access to information, deny access to information, cause disruption or damage to a device or network, or otherwise interfere with the security/privacy of users.
Verifiability	A term used in the context of elections to describe voting systems that produce robust evidence that votes in an election were not tampered with and the counting of votes is correct.
Ballot secrecy	A property of a voting system where each voter's choice is private.

Chapter 1

Introduction

1.1 Background

Online voting can allow voters to vote at home, from their personal devices, using an app or a web browser.

Adoption of this technology has generally been subject to much academic and political debate. On one hand, online voting offers much promise, as it can make voting more accessible to voters and increase participation. While the effect of online voting on voter turnout is difficult to measure, a 2018 study found that the adoption of online voting by Ontario municipalities could have increased turnout by 3.5 percentage points [33]. On the other hand, the use of this technology also creates new risks. The elimination of the paper ballot could disenfranchise voters who are uncomfortable voting online. The cybersecurity of online voting is also a major concern, as online voting systems may have a central point of failure, have weak authentication, have results tampered with, or experience outages, which can affect public trust in elections. Finally, a key principle of fair elections in Canada is that election results can be independently verified by observers, something that could be difficult to do depending on the implementation of an online voting system.

Ontario stands as a case of a jurisdiction that has conducted online voting at the municipal level for decades with little academic study and political debate. Municipal staff in Ontario could be motivated to adopt online voting because it can reduce the cost of administering elections. A 2017 purchase agreement for one municipality indicated the cost of online voting to be just \$1.40 per voter [18]. The province has conducted online elections since 2003, and as success stories were shared widely at municipal conferences and local associations of municipalities [33], the proportion of cities conducting online voting has increased rapidly. There are serious stakes: these local elections are sometimes hotly contested, and elect representatives who govern everything from cities to townships to school boards. The larger of these

organizations can have annual budgets upwards of CAD 500M.

Comparisons of cybersecurity risk have been made between online voting and online banking by municipal officials, but these technologies have differing cybersecurity challenges and tolerance to risk. With online banking, information about a customer's identity is linked to that customer's transactions, and fraud can be detected and disputed. Banks can automatically detect fraud by monitoring the behaviour of their customers, and customers can detect fraud by noticing transactions that they did not make. Customers can additionally be required to use 2-factor authentication with their mobile device. But with online voting, secrecy is a legal requirement and voter identities can not be linked to their choices. Universal suffrage (the right of all eligible voters to vote) precludes security features that would require voters to have a mobile device. These constraints, among others, make it a technical challenge for voters and online voting providers to detect errors or fraud. [12]

Ontario now represents one of the highest concentrations of online voting globally. Although turnout by voting method is not generally published by municipalities, a recent study estimated about 3.8 million voters were eligible to vote online in the 2022 Ontario municipal election cycle [32].

1.1.1 No Standards for Online Voting in Ontario Municipalities

There are currently *no* federal or provincial standards or guidelines for the implementation of online voting, including no requirements surrounding certification, testing, or, crucially, auditing. Instead, Ontario cities are given broad leeway to adopt, procure, and deploy this technology based on their own internal (and largely non-public) deliberations. Local officials create and apply their own cybersecurity requirements with varying degrees of success.

1.2 Problem Statement and Thesis Outline

A research gap exists for online voting in Ontario. While our literature review will show some important foundational work done in Ontario, two key questions remain largely unanswered:

1. Do security vulnerabilities exist in online voting technology used in Ontario?
2. How does the use of online voting technology in Ontario compare to other robust democracies that are using online voting?

To address these questions, this thesis is organized as follows:

Chapter 2 provides important legal, procedural, and technological background knowledge on the use of online voting technologies in Ontario and other jurisdictions. It also defines key verifiability requirements that academics have proposed for e-voting technology, as well as new classes of security threats that exist in the online voting context.

Chapter 3 presents an in-depth investigation into a novel ballot secrecy vulnerability for a particular online voting system in Ontario, and our attempts at sharing this vulnerability with other vendors that are active in Ontario

Chapter 4 presents a broad standards-based review of the use of online voting technology in Ontario to highlight the divergence between Ontario and other jurisdictions and to explore where and why these divergences exist.

Chapter 5 contains a discussion of selected findings, topics for future work, and a conclusion.

1.3 Thesis Contribution

The research contributions of this thesis are summarized below.

1. We present a novel ballot secrecy attack based on network traffic analysis of (encrypted) ballot confirmation pages. For a recent mayoral race in Canada, we demonstrate a classifier that could have correctly guessed voting intention for 84% of ballots based *only* on the byte length of encrypted network traffic.
2. We performed a detailed analysis of a real-world online voting system demonstrating the attack's effectiveness in spite of well-configured TLS and variable-length HTML/DOM elements. The latter differentiates our work from length-based attacks identified by Specter et al. as well as Clark and Essex [17, 51].
3. We made elections more secure for over 700,000 eligible voters in fifty Ontario municipalities by responsibly disclosing the vulnerability and collaborating with the impacted vendor to fix the vulnerability before the 2022 Ontario municipal elections.
4. We identified systemic problems with the cybersecurity vulnerability reporting process for online voting vendors that serve Ontario municipalities.
5. We performed the first standards-based analysis of online voting systems and related practices in Ontario and discovered major divergences between practices in Ontario and other robust democracies implementing online voting.
6. We proposed several recommendations on how to improve online voting in Ontario.

1.4 Thesis Statement

Online elections in Ontario lack the standardization, transparency, accountability, and verifiability that exists in other robust democracies that use this technology.

Municipal elections with e-voting in Ontario are largely privatized and lack transparency. In 2022, six private vendors designed, built, maintained, and operated online elections systems which were offered to municipalities as turnkey solutions. These vendors offer differing products: some with elements of verifiability, others with none. Access-to-information law can allow researchers to compel the release of important election-related documents from municipalities. However, this law does not apply to these private vendors, many of whom refuse to collaborate with security researchers.

Online voting presents numerous severe and catastrophic cyber-risks to municipalities. One such risk is that, depending on the implementation of the online voting system, it is possible to tamper with the election results in a way that is difficult to detect. Even if a result has not been tampered with, an allegation of tampering could be fatal to the perceived legitimacy of an election, especially with online voting systems that do not provide robust evidence of correct results.

Security researchers and cryptographers have made many proposals to avoid, mitigate, and provide contingencies for these risks, as well as others. Some jurisdictions have even required these proposals to be implemented by law. However, the systems used for online voting in Ontario often do not even *attempt* to implement these proposals. Even in cases where some security mechanisms are used, security vulnerabilities have been found by researchers. It is likely that undiscovered vulnerabilities persist, given that many vendors do not cooperate with security researchers.

Municipalities themselves have varying capabilities. Some municipalities that use online voting have less than 1000 electors and have limited budgets. With no dedicated Information Technology staff and no legislative or regulatory guidance from the province or federal government, these small municipalities must either take security claims of vendors at face value or informally collaborate with other municipalities to evaluate cyber risks. Other municipalities have admitted to not having cyber-incident response plans for their online elections, with one city clerk stating in 2018 that “We’re hoping nothing does happen” and another stating “I don’t have a disaster plan in place right now, I’d have to talk to my vendor about that.”¹

Major cybersecurity incidents in Ontario municipalities, even during elections, have not led to significant changes. A major outage on election day of e-voting services in 2018 did not have an impact on the adoption of e-voting, and the uptake of online voting has continued

¹<https://www.cbc.ca/news/canada/london/london-ontario-online-voting-1.4598787>

despite multiple ransomware attacks targeting municipalities in Ontario. These incidents have not prompted provincial or federal regulations for this rapidly growing sector.

Ultimately, this work shows that Ontario municipalities generally have done little to prevent or prepare for a potentially catastrophic cybersecurity incident in an online election. The many risks inherent to online voting remain unaddressed and unmitigated in Ontario, with little oversight, regulation, and transparency.

Chapter 2

Related Work

2.1 Online Voting in Ontario

The province of *Ontario, Canada* consists of 444 municipalities distinguished across upper-, lower-, and single-tier categories. However, only the lower- and single-tier municipalities conduct elections. Of these 417 municipalities, 217 (52%) offered an online interface to receive and cast a ballot in the 2022 Ontario Municipal Election, an increase of 42 cities over the prior 2018 election.¹

2.2 Principles of the Municipal Elections Act (MEA)

As part of their research into the 2018 municipal election cycle, Cardillo et al. studied the legal principles of online voting in Ontario. Their work states that the Municipal Elections Act (MEA) governs municipal elections in the province of Ontario [1]. This legislation allows for municipalities to authorize the use of alternative, remote voting methods (which implicitly includes online voting), but does not provide any specific guidance for municipalities to conduct online elections [12].

Despite this lack of clear guidance, Cardillo et al. stated that six key general principles of the MEA were outlined in *Cusimano v. Toronto* [37], which would apply to all methods of voting. Of these six principles, four are listed in Table 2.1 because they have particular relevance to this thesis, which explores ballot secrecy, availability, integrity, and verifiability in the online voting context in Ontario.

Cardillo et al. found that several of these principles in Table 2.1 may have been contradicted in the 2018 municipal elections. Availability is a major concern: many municipalities

¹2022 Municipal Election. Association of Municipalities of Ontario. Available: <https://www.amo.on.ca/municipal-election-statistics>

Summary	Principles identified in <i>Cusimano v. Toronto</i>
Ballot Secrecy	The secrecy and confidentiality of the voting process is paramount.
Availability	The election shall be accessible to the voters.
Integrity	The integrity of the process shall be maintained throughout the election.
Verifiability	There is to be certainty that the results of the election reflect the votes cast. So far as reasonably possible, valid votes shall be counted and invalid votes rejected.

Table 2.1: Election Principles

encountered outages of their online voting systems on election night. Cities broadly offered voters online voting systems lacked verifiability: they did not provide objective evidence beyond their testimony that the result was correct. This lack of evidence makes integrity issues difficult to detect if they exist:

Our observations point to what we believe is a serious concern over the degree of certainty of results achievable in the current online voting setting. If there ever was evidence of an incorrect result or fault (whether due to error or otherwise), some of the experiences we heard suggest that it would exist beyond the reach of the public.

Finally, online voting services used the voter’s date of birth as a credential. In smaller municipalities, many voters had unique dates of birth. This raises ballot secrecy concerns: Despite attempts made to de-identify voters in the online voting process, many voters could be uniquely re-identified by voting services because they had unique birthdays. Some of these examples will be expanded on in depth in Section 2.5.

2.3 Verifiability

2.3.1 Definition

Generally speaking, the term “verifiability” is used in the context of online voting to describe voting systems that produce robust evidence that votes in an election were not tampered with and the counting of votes is correct. Cortier et al state that verifiability is divided into three sub-properties: individual, universal, and eligibility verifiability [19]. It is important to note that not all voting systems that claim to be verifiable implement all of these properties.

Individual Verifiability

Individual verifiability allows a person to verify their vote was cast as intended. Cardillo et al. demonstrated that a malicious browser plugin could swap votes, causing a voter to unintentionally cast a ballot for the wrong candidate [12]. Individual verifiability can protect a user against this type of attack where the voter’s device is corrupted [19].

Universal Verifiability

Universal verifiability allows a person to verify that all cast votes were counted and that the count is correct. This can allow for independent discovery of a compromised voting server or an election authority reporting incorrect results, whether by malice or a transcription error. Often, this is done by providing a publicly accessible bulletin board that contains all votes. Using this bulletin board, a voter can find their vote on the board and total the results themselves to see if their vote is counted correctly [19].

Eligibility Verifiability

Eligibility verifiability allows a person to verify that no invalid votes were cast, and protects against attacks such as a compromised voting server “stuffing the ballot box” to add fictitious votes that support a candidate [19].

A notable example of eligibility-related abuse incorporating individual and universal verifiability was the Currin Trading Ponzi scheme in the video game *EVE Online* [47]. In this scheme, there existed a public bulletin board of investors, where any individual investor could verify their investment on the bulletin board as well as calculate the total amount invested. The administrator of Currin Trading described these mechanisms:

I decided that a useful tool for the site would be a “current accounts” section with a spreadsheet detailing the amount a person invested, when it was scheduled to mature, and for how much. I could make such a spreadsheet both public and secure: an account was identified only by a code name, so only the account holder would know whose it was. **Best of all, I could create dozens of fake accounts, supposedly investing billions, and no one could verify that these were not real investors.**² There would be a variety of investors putting in varying amounts, and for various periods on various days. I made sure that the first investor listed would have a long-term investment starting from December and going on into April, to heighten the illusion of a business that had been running a long time. Looking at

²Emphasis added by the author.

the investment information would be convincing. And once a real investor invested and got his account info posted to the spreadsheet among so many others, how would he ever suspect that his was the only real one among so many fakes³?

While not an online voting scheme, this had individual and universal verifiability mechanisms that resembled one. Despite these mechanisms, a lack of eligibility verification (ensuring that all records on a bulletin board are legitimate) allowed the administrator of this scam to “stuff the ballot box” with fake investors. This risk extends to the online voting context: the Belenios team argues that the Helios voting system provides individual and universal verifiability, but is still be vulnerable to “ballot stuffing attacks,” where a dishonest bulletin board could add fictitious votes to the list and alter the result without detection [19].

2.3.2 Additional Requirements

Benaloh [10] argues that verifiable voting systems must always protect the secrecy of a voter’s choice. Systems that produce evidence of a voter’s choice are advantageous because they allow voters to verify that their vote was cast as intended, but if this system allows voters to prove who they voted for to third parties, it also allows for coercion and vote-buying, which can affect the legitimacy of an election. For that reason, coercion-resistance and ballot secrecy are argued to be closely related essential requirements of verifiable voting systems. Not all voting systems that claim to be verifiable meet these requirements.

Ballot Secrecy

Ballot secrecy is a fundamental principle of democratic elections, and is a requirement in the 1948 Universal Declaration of Human Rights. It preserves privacy and offers protection against coercion, intimidation, and vote-buying [28]. As Elkit and Manley argued in 2019, a paper ballot cast at a polling station provides the firmest guarantees of secrecy:

Through its management of polling stations, the electoral administration takes responsibility for providing compartments in which the voter can vote alone; for ensuring that voters are not accompanied to these compartments by others except as authorized by law; and, in the case of a paper ballot, for ensuring that voters do not display their marked ballots before casting them. Where provision is made for political-party agents to witness the polling, this gold-standard scheme, properly

³<https://web.archive.org/web/20130118122617/https://www.themittani.com/features/ancient-history-currin-trading-confession>

implemented, will provide for balloting that is not only secret but is transparently so, with observers able independently to affirm that secrecy has been protected.

Ballot secrecy must also be ensured when election results are reported, as it is possible for sufficiently granular results reporting to violate a voter's privacy. For example, if all voters in a Canadian subdivision vote for the same candidate, the disclosure of the results of the subdivision will reveal the choices of individual voters. In Canada, Elections Canada addresses this through procedural and legal mechanisms:

On Election Night, when results are initially entered into the Event Results System, the program identifies all polls with Secrecy of the Vote issues. At Validation, Returning Officers are instructed to combine votes cast for any single candidate with those for the same candidate of another polling station. . . . With there being several reasons to combine two or more polls, not even electors who voted at that polling station, nor individuals with access to the List of Electors, could assume with any certainty that a secrecy issue was the cause. Elections Officers must sign a Solemn Declaration, which includes secrecy of the vote, so the limited few with knowledge of the issue are required, by law, to maintain the secrecy of the vote [27].

Recall that individual verifiability produces evidence that a voter's vote was cast as intended. Clark argues that verifiability mechanisms such as these must not compromise a voter's secrecy—a voter must be able to verify their vote was cast as intended, without being able to prove how they voted to a third party. [16]. The verifiability features of several e-voting schemes (Helios, Belenios, etc) do not protect against such ballot secrecy violations, but this is the aim of some verifiable voting schemes like Civitas [19].

Coercion Resistance

An adversary may attempt to coerce voters to influence an election result. In Canadian federal elections, voters use a hand-marked paper ballot to cast their votes. These elections have two procedural and one legal mechanism to prevent coercion of voters.

- Voters cast their ballot behind a privacy-protecting screen.
- Ballots cast with identifiable marks must be rejected.
- Intimidation, bribery, and attempts to violate ballot secrecy is an offence under the *Canada Elections Act*.

Elections Canada states these measures exist “to ensure that no electors are intimidated or bribed into voting in a particular way.” [26]

Clarke argues that ballot secrecy is critical to ensure coercion resistance. It is important to note that online elections often allow people to vote from home, on their personal device, which allows adversaries to violate ballot secrecy by shoulder-surfing voters. Some systems address this risk by allowing multiple voting.

2.3.3 Proposed and Implemented Verifiable Voting Systems

Verifiable voting systems have been proposed and/or implemented for in-person voting, postal voting, and online voting.

Essex and the Scantegrity team implemented an individually and universally verifiable system for optically-scanned paper ballots which was used in the 2009 municipal election in Takoma Park, Maryland [29]. Crimmins et al. proposed RemoteVote and SAFE Vote, two individually and universally verifiable systems for postal voting [20].

Verifiable systems have also been proposed for online elections as well. Belenios is an open-source online voting platform that has universal, individual, and eligibility verifiability [19]. Switzerland’s standards require that online voting systems have universal, individual, and eligibility verifiability.

2.4 Types of Threats to Online Voting

When compared to in-person, hand-counted, paper ballots which are chiefly verified through procedural measures, online voting presents new risks in existing categories of election threats. These threats fall into several categories:

- Ballot secrecy threats, where a person could determine how another person voted in an election.
- Coercion threats, where a voter is illegally pressured or incentivized to cast a particular vote.
- Count-related threats, where votes are counted incorrectly, or an incorrect count is reported.
- Ballot-stuffing threats, where invalid votes are cast and counted.
- Ballot-altering threats, where a voter’s choice is changed without their authorization.

- Authentication threats, where unauthorized individuals can cast votes on behalf of others.
- Availability threats, where access to the voting service is disrupted for voters.
- Privacy threats, where personal information about voters is accessed without authorization.
- Legitimacy threats, where the public does not have confidence in the election result.

2.4.1 Attackers

Attacker goals can include altering the result of an election, preventing some or all voters from casting a vote, and/or creating doubt in the validity of the election result. They may use a combination of threats to achieve these goals.

There is a broad list of potential attackers for municipal elections in Canada. Potential attackers could be politically motivated and desire a particular election outcome. Attackers could include partisan individuals/groups, people with a financial interest in municipal policy, or even state actors. The Canadian Security Intelligence Service has identified foreign interference as a threat at all levels of government, including the municipal level [50]. Potential attackers may also be financially motivated (e.g. a ransomware group targeting municipal infrastructure), or personally motivated (e.g. a disgruntled employee seeking to cause disruption).

In some cases, cybersecurity incidents may occur without an attacker (e.g. via human error or negligence). For example, unanticipated demand on an online voting system could cause an availability threat, or a political candidate could cause a privacy threat by leaving a USB flash drive containing voter data on a bus seat.

2.4.2 Technical Infrastructure for Online Voting

Online voting systems used in Ontario are web applications that generally have the following key components:

Voting Client & Voter Device

The voting client consists of the HTML, CSS, and JavaScript that is served to the voter's device.

At a minimum, the voting client is responsible for providing a user interface to voters for authentication and recording/casting their votes. It communicates with the voting server when doing so.

The voter device is the device used by the voter to cast a vote, which could be the voter's personal device, a shared household device, or a municipal device available in a voting location.

The voter device also includes non-voting-client software like the operating system and other installed applications.

Malware installed on the voter device could alter a voter's vote (ballot-altering threat), prevent the voter from accessing the voting service (availability threat), or share the voter's candidate choice with others (ballot secrecy and coercion threats). If malware is detected on a municipal device used as a voting kiosk in a voting location, it could also raise a legitimacy threat.

If a voter can access the voting client in a place without guaranteed secrecy (like their home), coercion and ballot secrecy threats exist, as voters can be shoulder-surfed by others in that location.

Administrator Client & Administrator Device

The administrator client consists of the HTML, CSS, and JavaScript that is served to an election administrator's device and accessed in the election administrator's web browser. It also includes the election administrator's device and all software running on that device.

At a minimum, it is responsible for providing a user interface to voters for election administrators to see relevant data about the election and report the results of the election. It communicates with the voting server when doing so.

The administrator device is the device used by the election administrator to use the administrator client. Depending on municipal policies and practices, this may be a municipally managed device, a personal device, or a shared device (e.g. a household device or a municipal device with multiple authorized users).

Malware installed on the administrator device could change the appearance and contents of the administrator client, causing an incorrect election result to be reported (count-related threat). It may also grant an attacker access to personal information about voters (privacy threat).

Voting Server

The voting server is generally responsible for serving the client application to the voter, serving the client application to the administrator, authenticating voters, performing various administration tasks (like generating reports), counting votes, and reporting the total.

The voting server may consist of multiple components that run on different servers, which is a requirement of the Swiss OEV. Alternatively, the server application may be a single monolithic application, or even depend on a blockchain.

Unauthorized access to a voting server or malware installed on this server could present

several risks, depending on the design/implementation of the voting system. These include ballot-stuffing threats, count-related threats, ballot-secrecy threats, ballot-altering threats, authentication threats, availability threats, and legitimacy threats.

Network Path

Data is sent and received from the voting client/administrator client and voting server via the Internet. Because Internet infrastructure could be compromised by malware and is operated by third parties including Internet Service Providers (ISPs) and nation-states, it is not inherently considered trustworthy. Communication can be eavesdropped on or altered by a malicious device in the network path.

Online voting providers address this by, at minimum, ensuring data is encrypted with Transport Layer Security (TLS), which is a typical security precaution for most websites. Some online voting providers also use client-side JavaScript to perform additional encryption.

Regardless of the use of TLS, a malicious device in the network path is still capable of blocking a connection to the voting server (availability threat).

Note: Our research in Study 1 finds that in some cases, encrypting data with TLS is not a sufficient precaution to preclude ballot secrecy threats, and our research in Study 2 shows that TLS alone is insufficient to prevent ballot-altering or authentication threats

DDOS Protection Providers

Many online voting services rely on third-party providers like Cloudflare to protect against Distributed Denial-of-Service (DDOS) attacks. With these services, the voting client connects directly to a server operated by the DDOS mitigation provider. The provider may require the voter to enter a CAPTCHA to access the voting service. Once the voting client is authenticated by the DDOS mitigation provider, the DDOS mitigation provider relays communication between the voting client and the voting server. This practice can protect voting servers from DDOS attacks, which is a type of availability threat.

However, depending on configuration, using these providers can create new ballot secrecy and ballot-altering threats [21].

Third-Party Software

Third parties beyond the voter, administrator, voting server, and network path are also key parts of online voting infrastructure.

One such way a third party can be part of online voting infrastructure is through JavaScript or styling dependencies which are loaded by the voting client. These dependencies, such as

JQuery and Bootstrap, allow developers to write less code to achieve the same task, but it requires clients to load these dependencies. These dependencies may be served directly from a third-party server or may be served from the voting server. Our passive investigation of Ontario's e-voting systems in Study 2 found many vendors use third-party client dependencies, sometimes loading a local copy of this dependency from the voting server, sometimes loading directly from a third-party server, and other times loading directly from a third-party server with an integrity check, which can prevent the dependency from being included if a change is detected.

Finally, third-party software is almost certainly included in the voting server. Third-party software includes the operating system (Windows, Linux, etc) as well as other applications and dependencies that are running on the server that were not developed by the online voting vendor.

To summarize, this third-party software can affect the voter client, administrator client, and voting server. Because malware can be surreptitiously included in this third-party software⁴, the use of third-party software creates ballot-secrecy, count-related, ballot-stuffing, ballot-altering, authentication, availability, privacy, and legitimacy threats.

2.5 Illustrative Examples of Online Voting Threats Relevant to Ontario

This section contains real-life examples of specific threats that have particular relevance to e-voting in Ontario.

2.5.1 Flawed Verifiability

Flaws in verifiability mechanisms could allow adversaries to provide false proofs of a different election outcome, reveal the choices of individual voters, and/or allow adversaries to coerce voters.

Example: 2019 SwissPost/Scytl vulnerability. Security researchers examining the source code of the online voting system being certified for use in Swiss elections discovered a major vulnerability in the system's universal verifiability mechanism. This vulnerability could allow a malicious elections authority to provide a tampered proof for an altered election result that would be "perfectly indistinguishable" from a truthful proof [23].

⁴One recent and topical example is the xz vulnerability discovered in March 2024 <https://nvd.nist.gov/vuln/detail/CVE-2024-3094>

2.5.2 Insufficient Evidence

Alternatively, online voting systems with no verifiability mechanisms and/or tamper-proof logging lack the evidence of correctness or wrongdoing created through procedural measures of a well-administered in-person, hand-counted election. This could make claims of fraud difficult to disprove, even if no fraud took place. Likewise, it could make fraud difficult to detect, and if detected, difficult to investigate.

Example: 2017 United Conservative Party Leadership Race. The Alberta Royal Canadian Mounted Police (RCMP) investigated claims of voter fraud in this election, which was conducted through an unverifiable online voting system. This investigation identified “suspicious” votes by interviewing individuals who claimed that votes were cast on their behalf and/or where multiple votes were cast from the same phone number and/or IP addresses [49]. The investigation concluded that there were “less than 200” “suspected instances of potential identity fraud.” At a press conference, an RCMP spokesperson acknowledged that it was difficult to gather sufficient evidence to lay charges because it can be impossible to know what device is connected to a suspected instance of fraud:

We have evidence to suggest there is potential fraud in the case of those votes, but it’s important to clarify... ..there was insufficient evidence to lay a charge and our biggest obstacle was being able to satisfy ourselves that we would have sufficient evidence around the identity of the persons responsible to prove that. And when you think about how [online] voting works, you need a witness often to an offence. **And if you don’t have a witness you need to tie the device that was connected the offence, if it’s even knowable, because there’s ways sometimes it’s not knowable...**⁵ ... we didn’t have that evidence at the end of the day [48].

2.5.3 Weak Authentication Credentials

Weak voter authentication credentials could enable an unauthorized party to cast a ballot on behalf of another voter.

Example: 2018 Ontario municipal elections. In many municipalities, voters were mailed informational letters that contained instructions on how to vote along with their voting credentials. Voters were asked to input these credentials, using their birthday as an additional form of authentication. Cardillo et al. demonstrated that in some municipalities, it was possible to read these credentials without opening envelopes by holding them up against a light [12]. Using a

⁵Emphasis added by the author.

birthday as an additional form of authentication is a weak second factor: Dates of birth can be known by household members of voters, and are not considered secret by all levels of government. For example, the Ontario COVID-19 vaccine passport QR code contained the name and date of birth of Ontario residents.

2.5.4 Client-side Vote-altering Malware

Malware installed on voter devices could alter votes before they are sent to the voting server.

Example: 2014 independent security analysis of Estonian online voting system. This analysis demonstrated a credential-stealing client-side malware that could replace a voter's vote without detection [34].

2.5.5 Client-side Count-altering Malware

Depending on the e-voting system, malware installed on administrator devices could create count-related risks.

Example: Malware on devices of municipal officials. While vote-total-altering malware has not been detected on the devices of municipal officials, recent incidents may indicate that municipal infrastructure in Ontario is vulnerable to malware. In 2024, Huntsville⁶ and Hamilton⁷ suffered from ransomware attacks. Another three cities (Wasaga Beach, Stratford, and The Nation) that used online voting in 2018 had ransomware attacks. The former deputy director general of the scientific and technical services branch of the Canadian Security Intelligence Service (CSIS) stated in a 2022 interview that “The attack surface of municipalities remains critically high. Looking at the raw data, I am not sure things are getting better [9].”

2.5.6 Unauthorized Access to Voting Server

General web security vulnerabilities of online voting system server software or infrastructure, if exploited, could allow attackers to violate ballot secrecy or alter vote totals during an election.

Example: 2010 Washington, DC online voting pilot project. Security researchers from the University of Michigan exploited a code injection vulnerability to reveal the names of voters and their choices as well as change every vote [34].

⁶<https://globalnews.ca/news/10353659/second-ontario-municipality-reports-cybersecurity-incident-within-three-weeks/>

⁷<https://www.cbc.ca/news/canada/hamilton/ransomware-attack-1.7133457>

2.5.7 Online Voting Website Outage

Downtime of online voting systems is an availability risk that could disenfranchise voters. If voters become habituated to downtime in online elections, it could also mean that selective downtime targeting some voters to influence a result is less detectable.

Example: 2018 Dominion outage. In Ontario’s 2018 municipal elections, 43 municipalities using Dominion Voting Systems’ online voting service experienced voting outages on election day. Because many affected municipalities did not offer a paper alternative to online voting, their officials were left with no choice but to declare emergencies and extend the voting period by as much as 24 hours [36]. The cause of the outage was later described as a “miscommunication between Dominion and the service provider” where the service provider placed a too-restrictive cap on the bandwidth usage of Dominion’s online voting system [12].

2.6 Online Voting in Other Jurisdictions

Estonia has offered online voting in national elections starting in 2005, and Switzerland has offered it sub-nationally since 2003 [31]. Over 300,000 Estonians (representing over half of participating voters) cast a ballot online in the 2023 Parliamentary elections.⁸ And over 650,000 online voters participated in the 2021 State election in New South Wales (Australia).⁹

2.6.1 Regulatory Safeguards

Council of Europe’s Standards of E-Voting (SeV)

The Council of Europe’s Standards of E-Voting (CoE SeV) is described as “the main international legal standard in the field” by Rodríguez-Pérez [46]. Building on a minimal set of recommendations given in 2004, the 2017 CoE SeV contains a broad mix of technical, procedural, and regulatory requirements to ensure that e-voting respects all principles of democratic elections.

However, Rodríguez-Pérez argues that the SeV’s provisions regarding secret suffrage are flawed. He argues that guidance is missing to ensure whether or not cryptographic mechanisms to preserve ballot secrecy are safe from quantum computers. He also argues that the standard contains requirements based on unhelpful analogies to paper-based voting systems that don’t reflect the state of the art in e-voting. For example, homomorphic tallying of votes makes some

⁸<https://valimised.ee/en/archive/statistics-about-internet-voting-estonia>

⁹<https://elections.nsw.gov.au/About-us/Media-centre/News-media-releases/iVote-and-2021-NSW-Local-Government-elections>

data separation requirements in the SeV unnecessary. Additionally, he addresses the problem of voting in uncontrolled environments, where an adversary can shoulder-surf a voter. Other jurisdictions, like Estonia and Norway, allow for multiple voting (where a voter may cancel their vote and vote again later) to mitigate this concern, but such mitigations are not required in the SeV. [46]

Swiss Federal Chancellery Ordinance on Electronic Voting (OEV)

The Swiss Federal Chancellery Ordinance on Electronic Voting (OEV) is a legally binding standard that governs online voting in Switzerland. The OEV is more detailed than the CoE SeV and contains several hundred requirements. It rigidly defines the system architecture of e-voting systems, describes thirty-eight specific threats that must be addressed in risk assessments, and details specific requirements for operating manuals [53]. It even contains requirements for source code quality/modularity, reliable and verifiable compilation, and quality assurance. One such example is 25.11.3 of the OEV, which specifies that “The source code does not contain any superfluous variables.”

These ordinances exist in the context of a single open-source voting system being developed by the national postal service of Switzerland and consider private sector involvement a risk. For example, 2.9.3.3 of the OEV states that “If an entire group of control components is used by a private system operator, none of these control components is considered trustworthy” while 3.1 states:

The operation of the set-up component and at least one control component in the group which contains part of the key for decrypting the votes is the **direct responsibility of the canton and must take place within its infrastructure. Outsourcing to a private system operator is not permitted.**¹⁰

This contrasts with practices in Ontario, where private system operators are considered trusted.

A caveat is that these ordinances should be understood as specific to the Swiss context. For example, universal verifiability in its strictest sense (where any interested individual may verify the result) is not required—instead, specifically appointed auditors verify the results of elections.

¹⁰Emphasis added by the author.

Chapter 3

First Study: Discovery, Analysis and Mitigation of a Ballot Secrecy Vulnerability in a Real-world Election System

3.1 Introductory Remarks

In this chapter, we examine the question of ballot secrecy from the network perspective: Specifically, we explore whether a network-based observer can extract information about voter selections from the length of the exchanged network data. Although ballot secrecy is a well-established requirement of democratic elections, the online voting setting offers new opportunities for exploitation. For example, suppose a network observer such as an internet service provider, content delivery network, or data center could determine how you voted. In that case, they could selectively prevent your ballot from reaching the election server to unduly influence the outcome of the election. Worse, with growing precedent for service disruptions and outages due to inadequate bandwidth¹ on election night [12], a deliberate attack of this attack could escape detection.

Our analysis consists of a detailed analysis of the Simply Voting implementation, which had randomly varying lengths of exchanged data due to dynamic page content and gzip compression. We demonstrated that we could correctly guess a voter's selection with accuracy values ranging up to 100% in some instances. Even on more complex ballots, we generally

¹<https://zdnet.com/article/no-surprise-nsw-ivote-fails-during-local-council-elections/>

could still rule out some combinations of candidates. We conducted a coordinated disclosure with the vendor and worked with them to roll out a mitigation.

To their credit, this discovery (and therefore its fix) was made possible by their willingness to provide a *publicly* accessible demo, which, as we will show, remains a rarity in the industry. The rest of the chapter is organized as follows: **Section 3.2** presents background and related work. **Section 3.3** recounts our efforts to reach out to vendors to seek demos for their voter interface. **Section 3.4** describes the basics of the Simply Voting system. **Section 3.5** describes our overall testing methodology, including technical details of our approach replicating Simply Voting’s server functionality and collecting network data. **Section 3.6** presents the results of a simple (single contest) attack on ballot secrecy. **Section 3.7** extends the experiment to more complex ballot configurations. Finally, **Section 3.8** describes our coordinated disclosure with Simply Voting, their mitigation strategy, and the approaches of the other (responsive) vendors.

3.2 Background and Related Work

Ballot secrecy in online elections has been studied in the context of active attacks, such as subverting TLS [13, 35], exploiting implementation vulnerabilities [52, 56], or by unacknowledged privileged access [22]. Little related work has evidently explored passive attacks that focus on the *lengths* of exchanged messages. One of the first articulations of this risk is a requirement due to Volkamer and Krimmer [55] (emphasis added):

The e-voting system SHALL ensure neither the vote itself nor the number of chosen candidates (including an empty ballot), nor a spoilt vote (eg, by using the length of the protocol messages depending on the approach) can be deduced by reading transmitted voting protocol messages.

Clark and Essex [17] considered the possibility of a network observer being able to differentiate a voter’s selection based on the length of encrypted traffic sent to the election server by the voter’s browser. They found Dominion Voting Systems encoded candidate names explicitly in the cast vote object. For example, they observed a vote for *Meghan Agosta* was sent in an (encrypted) POST as {"ChoiceName": "Meghan Agosta"}. They speculated this approach could be susceptible to network-based length attacks, but did not conduct an analysis.

More recently, Specter et al. [51] explored this question in the context of the Voatz mobile voting app. Like the Dominion example, Voatz explicitly encoded the chosen candidate’s name, sending it to the server along with associated metadata in an HTTP POST. The authors observed a difference in the transmitted byte length of packets between a ballot cast for a candidate with a “short” name versus one with a “long” name.

However, our own experience examining online voting implementations has generally found cast ballot objects have a *fixed length*, with selections represented either as a code or ciphertext. This approach seemingly precludes length-based analysis—so we thought.

3.3 Research Question and Scope

Online voting systems typically display a confirmation screen allowing voters to confirm their selections before casting. Our study began with a hypothesis: Do these ballot confirmation pages leak information about a voter’s selections? In particular, if the page was generated at the server-side and sent to the client immediately prior to casting, the TLS record byte-length may reveal information about the selected candidate.

Testing this hypothesis required access to a real-world online voting implementation. However, we were unaware of any vendor who maintained a publicly accessible demonstration that we could examine. The sole exception we observed was Simply Voting, a Montreal-based online voting vendor. Simply Voting mostly focuses on *non-governmental* elections (schools, companies, unions, political parties, etc.), however, they did run the elections of 28 cities (accounting for over 300,000 voters) in the 2018 Ontario Municipal Election [12]. In 2022, they ran the elections of 50 municipalities².

3.3.1 Vendor Demo Access Requests

As explained in subsequent sections, we were able to confirm our hypothesis on Simply Voting’s demo website. But what about the industry at large? Following our coordinated disclosure with Simply Voting, we decided to reach out to companies who had run (or were likely to run) a civic election in the near term.

We emailed each company identifying ourselves as cybersecurity researchers requesting a demonstration of the ballot casting experience. For each vendor, we recorded whether they responded to our request, whether we were granted access to a demo, whether it was vulnerable to length-based analysis, and if so, what mitigation strategy was employed. We gave each vendor 30 days to respond. The results are shown in Table 3.1. The observed mitigations are discussed in Section 3.8.

²<https://www.simplyvoting.com/simply-voting-at-the-2023-amcto-conference/>

Table 3.1: Vendor responses to our demo request and associated findings.

	Responsive	Access Granted	Vulnerable	Mitigation Strategy
Dominion	No	No	Unknown	Unknown
Intelivote	No	No	Unknown	Unknown
Neuvote	Yes	Yes–Private	No	Client-side generation
Scytl	Yes	No ^a	Unknown	Unknown
Simply Voting	Yes	Yes–Public	Mitigated	Random-length padding
SwissPost	Yes	Yes–Private	No	Client-side generation
Voatz	No	No	Unknown	Unknown

^aAgreed in principle, but access not granted by time of writing.

3.4 Description of Simply Voting's System

This section describes Simply Voting's process for casting ballots and evaluates the possibility of a length-based inference at different parts of this process.

3.4.1 Ballot Casting Process

Step 1: Logging In. The voter navigates to `demo.simplyvoting.com` and logs in with the given user ID and password. The user's full name is then included in the HTML of the subsequent pages they access during the session.

Step 2: Submitting Choice of Candidates. The voter is presented with a single ballot page, which contains a set of offices (e.g., Mayor and City Councillor) and candidates. The voter selects which candidates they would like to vote *for*, and presses the **Continue** button. This submits a form containing the voter's choices to the server represented as fixed-length codes.

Step 3: Confirmation. A confirmation page is sent to the voter from `demo.simplyvoting.com`. The served HTML content of this page contains the voter's name, as well as the name of the voter's choice of candidate. Note that static content, like images, stylesheets, and scripts, is served from a different domain, `static.simplyvoting.com`, with a different IP address.

Step 4: Review and Submission. The voter may choose to go back to the previous page and change their choices. If they do, they will again be presented with a confirmation page. If they are satisfied with their choices, the voter clicks the **Confirm** button, and their ballot is submitted to the server.

3.4.2 Potential Side-channel Attacks in the Ballot Casting Process

One opportunity for a length-based attack is when a voter’s selections are sent to the server, as was observed in the Voatz system [51]. The names of the chosen candidate names were being POSTed to the server as explicit, uncompressed text. By contrast, Simply Voting’s system only POSTs fixed-length candidate IDs. For example, a vote for *Cassandra De Rolo* as Committee President is encoded in the HTTP request to the server as `ballot_579193[]=5724277`. Conversely, a vote for the opposing candidate, *Fernanda Rodriguez*, is represented by `ballot_579193[]=5724278`.

But what happens if the server returns a confirmation page containing the explicit names of the voter’s selections?

The values of some of the DOM elements are unknown to a network observer, while others can be predicted or deduced (see Table 3.2 for the full list).

We hypothesized that the length and value of the chosen candidate’s name had at least some effect on the size of the confirmation page and could leak information under certain conditions.

Table 3.2: Confirmation page DOM elements with varying values

Element	Example	Length	Predictable	Changes
CSRF Token	c9590a...67652	fixed	no	by session
Vote Serial	e600de...9683b	fixed	no	by session
Static Resource Version	84932	fixed	yes	weekly ^a
Text Time Remaining	5 minutes and 0 seconds	varies	likely ^b	every second
Integer Time Remaining	300	varies	likely ^b	every second
Voter Name	Taher Elgamal	varies	varies ^c	every voter
Chosen Candidate(s)	Linda Marlene Eales	varies	–	by ballot

^aUsed by Simply Voting to periodically invalidate browser caches of their static resources. We sampled it every few days during the testing period.

^bAn observer could reasonably guess this by applying an offset to the time observed on their own confirmation page. However, off-by-one errors are possible: to make our approach as conservative as possible, we do not rely on knowing the time in our testing.

^cCould plausibly be known by ISP or network administrator, see Section 3.5.3.

3.5 Methodology

To test our hypothesis that a voter’s choice could correlate to the TLS record length of the ballot confirmation page, we needed to make a large volume of requests for confirmation pages and analyze the data transferred. Simply Voting’s public demo of their service allows us to observe what data is transmitted from their servers in a realistic election setting. However, making

tens of thousands of requests to their servers would place an undue burden on their resources and could trigger their network intrusion detection systems. Instead, we created our own server that replicates their confirmation page functionality. We also designed an application that could automatically make thousands of browser requests to this service and log the response for later analysis.

3.5.1 Testing a Length-Based Side-channel Attack

We created a testing system composed of two parts: a Client Application (to mimic a set of voters) and a Server Application (to mimic the online voting system). Each ballot “cast” in the experiments below corresponded to an actual HTTP request made over the internet between our local Client and cloud-based Server applications.

We designed our applications to simulate an election where a voter is eligible to vote for one or more offices (e.g., Mayor, Councillor, Deputy Mayor) and may cast a vote for no more than *one* candidate for each office. A voter casts a single *ticket*, a combination of candidates selected for each office. This is a common electoral system for municipalities in Ontario. Some Ontario municipalities use at-large systems,³ but this chapter does not examine those elections.

3.5.2 Technical Implementation of the Client Application

We created the Client Application using Python, Selenium WebDriver, Google Chrome, and Wireshark. It was designed to make requests for confirmation pages, programmatically capture the response at the network layer, parse the TLS record length, and log the candidate choice and TLS record length to a file for statistical analysis. Our test bench is extensible and programmable: The client can decide which ballot to render by sending descriptive JSON to the server. The client can also set the flags to modify server behavior. For example, we implemented a flag that could programmatically enable/disable Simply Voting’s X-Ballot-Secrecy header (see Section 3.8.3).

The Client Application takes the following steps while interacting with the Server Application:

1. Client App is provided a list of offices and candidates (see e.g., Table 3.3).
2. Let o be the total number of offices and let $C_1, C_2 \dots C_o$ represent the set of choices available to a voter for each respective office (including abstain). The set of all possible candidate combinations (also known as *tickets*) that could be submitted by a voter T , is

³<https://guelph.ca/wp-content/uploads/Ward-councillors-or-councillors-at-large.pdf>

Table 3.3: 2018 Municipal Ballot Options in Ward Ennismore, Township of Selwyn

Mayoral Candidate	Council Candidate
Linda Marlene Eales	Donna Ballantyne
Andy Mitchell	Brad Sinclair
Ron Black	ABSTAIN
ABSTAIN	

$(C_1)(C_2) \dots (C_o)$. The Client Application generates $|T|n$ tickets, where n is the required sample size for each ticket.

3. In its main process, the client requests a ballot confirmation page from the Server Application using Google Chrome automated with Selenium WebDriver. The confirmation page contains one ticket in T . The main process of the Client Application then listens to a message queue.
4. A second process (the *listening process*) uses Wireshark's Python API⁴ to continuously listen to responses from the server application. When a response is detected, it records the TLS record length and pushes its value into the message queue.
5. The Client Application's main process receives a TLS record length from the listening process in the message queue. Each observed record length (and the associated candidate) is appended to a CSV file. Steps 3 to 5 are repeated $|T|n$ times until the test is complete.

3.5.3 Technical Implementation of the Server Application

Our goal was to replicate Simply Voting's confirmation page functionality as faithfully as possible. To that end, we studied Simply Voting's server stack and voting application by analyzing headers and interacting with their publicly accessible demo. We then matched this server stack as closely as possible, choosing popular and up-to-date software to fill gaps in the stack where Simply Voting's choice was unknown (e.g., the server OS).

Observing Simply Voting's Server Stack.

We used several methods to learn about Simply Voting's application configuration. We performed an SSL test⁵ to determine their supported and preferred encryption methods and ana-

⁴<https://github.com/KimiNewt/pyshark/>

⁵<https://www.ssllabs.com/ssltest/>

lyzed the server headers sent to us while interacting with the demo application. We were able to determine the following relevant information about their server configuration:

- `demo.simplyvoting.com` reports its server software is Apache
- The contents of the confirmation page are compressed via gzip
- The confirmation page is streamed to the client with chunked transfer-encoding. However, in practice, only one chunk is transferred.⁶
- The TLS cipher suite on Windows and Linux desktops running Firefox or Chrome is `TLS_AES_256_GCM_SHA384`.⁷

Approximating Simply Voting's Server Stack.

We rented a Virtual Private Server (VPS) from ChunkHost to use as our replicated voting server, connected it to a domain name, and obtained a TLS certificate from Let's Encrypt. We then deployed our Server Application with the following stack:

- **Debian 11.3 as the OS.** While we do not know what OS Simply Voting's servers use, Debian is an operating system with considerable market share in the server space, and 11.3 was the latest release at the time of writing.
- **Apache 2.4.52 as the server.** Simply Voting reported in its headers that it used Apache, and Apache 2.4 was the most recent minor version.
- **Flask/Python 3.9 as the web framework.** Simply Voting's web framework is unknown to us. For consistency with our client and analysis applications, we chose a Python-based web framework, and Flask is a mature Python web framework that met our relatively simple use case.
- **The TLS ciphersuite was forced to `TLS_AES_256_GCM_SHA384`.** This is the same as the TLS cipher suite preferred by Simply Voting on Windows and Linux desktops with major browsers.
- **Apache's HTTP response headers** were manually overridden to match to Simply Voting's.

⁶We tested chunked transfer-encoding on and found it made no significant difference in the ability to distinguish different ballots in our tests.

⁷The chosen cipher suite does not impact the feasibility of our attack. An observer can compute a separate record-length distribution for each observed cipher suite.

Replicating Simply Voting's Web Application.

Our Server System re-implements Simply Voting's ballot confirmation page. Upon receiving a request from the Client Application, the Server Application generates a confirmation page HTML document containing the data in Table 3.2, compresses it with GZIP, encrypts it with TLS_AES_256_GCM_SHA384, and serves it to the Client Application. Table 3.2 shows the elements with varying contents in the confirmation page, and our implementation substitutes appropriate values for all DOM elements with dynamic content:

- The Server Application generates random CSRF tokens and Vote Serials for each request.
- The Application assumes the Static Resource Version is fixed, as we observed it did not change for days at a time.
- The Server Application kept the voter's name static across our trials for several reasons. First, real-world municipal elections do not include the voter's name in the web session [12]. The voter's name may be present in non-civic elections (unions, student clubs, and political parties). Even in these cases, two further reasons exist for assuming the voter's name is known. First, the likely threat actors (e.g., internet service providers, family members, and cellular carriers) could plausibly associate a voter's TLS session with their identity and compute a distribution of TLS record lengths for a voter with that name. Second, to meaningfully abuse ballot secrecy vulnerabilities in many cases, it is necessary to already know the identity of the voter whose ballot is being observed.⁸
- The Application makes a conservative assumption that the time remaining varies within a 48- to 72-hour window before voting closes. A more sophisticated observer may be able to increase the accuracy of their predictions by building a distribution with a more narrow time window to better approximate when a voter casts a ballot.
- The Server Application inserts the candidate choice that is requested by the Client Application.


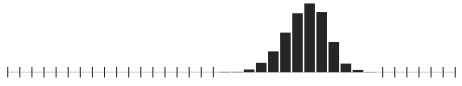


⁸In the case of a selective network outage attack, only the chosen candidate (not the voter's name) is relevant to the attacker.

3.6 Experiment 1 (Single contest): Township of Selwyn, Ward Lakefield

3.6.1 Data Collection

In our first experiment, we replicated the behavior of a simple confirmation page offering a single choice for a single office, with a substantial length difference for each candidate name. One Ontario municipality that used Simply Voting during the 2018 municipal election meeting this criterion was the Township of Selwyn.⁹ In 2018, voters in Ward Lakefield were eligible to vote for a Mayor, Deputy Mayor, and a Councillor. However, the positions of Deputy Mayor and Councillor were uncontested, so voters only cast a ballot for Mayor. Voters had four possible choices: Linda Marlene Eales, Andrew Mitchell, Ron Black, and Abstain.

Table 3.4: Observed TLS Record Lengths (2,000 trials per candidate)

Candidate	Frequency of Occurrence	Length (Bytes)		
		Min	Mean	Max
Abstain		3,301	3,306	3,311
Ron Black		3,319	3,326	3,331
Andy Mitchell		3,322	3,329	3,334
Linda Marlene Eales		3,327	3,333	3,338

Using our Client/Server test bench described in the previous section, we cast 2,000 ballots for each candidate: While we used the actual candidate names from this contest, we simulated an equal proportion of votes for each choice instead of the proportions of the actual election result. We recorded the TLS record length for each confirmation page returned by the Server Application. The distribution of TLS record lengths for each candidate choice is shown in Table 3.4.

⁹<https://elections.amo.on.ca/web/en/municipal/19401>

3.6.2 Data Analysis

We want to estimate the probability that an encrypted vote V with byte length B is for candidate k , i.e., $\pi(V_k|B)$. To classify which candidate the encrypted vote is for a given byte length, we choose the candidate who maximizes the posterior probability:

$$\begin{aligned}\widehat{V}_k &= \arg \max_{k \in K} \{\pi(V_k|B)\} \\ &= \arg \max_{k \in K} \{\pi(B|V_k)\pi(V_k)\}.\end{aligned}$$

Generally, $\pi(B|V_k)$ is unknown. However, we can use simplifying assumptions to facilitate prediction. In particular, if we consider byte length as a categorical variable, then we can assume the likelihood for byte length is multinomial

$$\pi(B|V_k) = \text{Multinomial}(\theta_k).$$

Here, the multinomial parameter θ_k is indexed by k to allow for different candidates to have different probabilities for observing various byte lengths. Making this assumption on the likelihood leads to the *Multinomial Naive Bayes Model*. We selected Naive Bayes since we could freely estimate $\pi(B|V_k)$ without making too many assumptions on the likelihood. Using data with labelled votes and byte lengths, θ_k can be estimated and then used to make predictions.

Using Python and `scikit-learn` [45], we ingest the data recorded by the Client Application and fit a Multinomial Naive Bayes Model and evaluate its out-of-sample performance on predicting which candidate a vote is for given the encrypted vote's byte length. To estimate our model's out-of-sample performance, we randomly split our data, using half to train the model and the other half to assess the accuracy of the model. The training set was used to fit our model. The performance metrics we present below are based on the predictions made on this test set.

We evaluate model classification ability using three metrics: accuracy, precision, and recall. The ballot in this example has four choices, and we simulated an equal proportion of results for each choice. This means that the best accuracy that should be achieved for a random guess—at least in theory—is 25%.

Result. The Naive Bayes model yielded an accuracy, precision, and recall on the test set of 83%, meaning 83 of every 100 votes from a simple random sample are correctly classified using byte length alone. Class-specific accuracy varies among candidates, with some candidates seeing very high accuracy (89%) while others see smaller accuracy (58%). However, accuracy across all classes is consistently larger than the expected 25%.

True Label	Abstain	1	0	0	0
	Black	0	0.86	0.13	.01
	Mitchell	0	0.26	0.58	0.16
	Eales	0	0	0.11	0.89
		Abstain	Black	Mitchell	Eales
		Predicted Label			

Figure 3.1: **Confusion Matrix (Proportions), Experiment 1.** Rows normalized to sum to 1. Diagonal entries indicate class candidate-specific accuracy, while the other cells indicate proportion of votes for row candidate predicted to be the column candidate. As an example, 86% of votes for Black were correctly predicted to be for Black. 13% of votes for Black were predicted to be for Mitchell. The remaining 1% of votes for Black were predicted to be for Eales.

Figure 3.1, the confusion matrix, shows details about the predictions made by the Naive Bayes model on our test set. Voter choices are ordered by their mean TLS record length: It is apparent that the model is only confusing voter choices that are closest to each other in mean length. This property proves useful in later analyses of more complex elections. See *Identifying a Subset of Possible Candidate Combinations* in 3.7.1.

3.7 Additional Experiments

We conducted additional experiments with more complex confirmation pages that contain voter choices for multiple offices.

3.7.1 Experiment 2 (Two contests): Township of Selwyn, Ward Ennismore

In 2018, voters in Ward Ennismore had four possible choices for mayor and three possible choices for Councillor, listed in Table 3.3. This results in twelve possible unique candidate

combinations (tickets). We collected 500 samples per combination, for a total of 6,000 samples. Fitting a Multinomial Naive Bayes Model, we find values for accuracy, precision, and recall in Table 3.5. In general, performance is lower than in Experiment 1 because the length variation of different confirmation pages for the same candidate is greater. The variation increases due to candidates for other offices being present on the confirmation page: they vary independently from the candidate being predicted.

Table 3.5: Performance on Test Set by Office, Experiment 2.

	Mayor			Councillor		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Naive Bayes	65%	75%	65%	50%	58%	51%
Random Guessing	25%	25%	25%	33%	33%	33%

Identifying a Subset of Possible Candidate Combinations. We also consider a more relaxed definition of violating ballot secrecy. Given a certain TLS record length, if we could identify a subset of possible candidate combinations that were chosen, that would also violate ballot secrecy. For each byte length, we counted the number of ballot configurations that produced record lengths of that byte length. Table 3.6 shows the proportion of ballots that have a TLS record length unique to a subset of possible candidate combinations.

Here, a possible candidate combination of n means that record length was sufficient to identify a vote to within n out of the 12 possible candidate combinations. Of note, 100% of ballots are associated with at most 11 possible candidate combinations, meaning that limited information about a voter’s choice is leaked for every ballot. In other words, for all ballots, we know at least one combination of candidates that were *not* chosen by the voter.

3.7.2 Experiment 3 (Three contests): Town of Ajax, Ward 1

In 2018, voters in Ajax Ward 1 had six possible choices for Mayor, three possible choices for Regional Councillor, and seven possible choices for Councillor, resulting in 126 possible candidate combinations. We collected 987–1052 samples for each combination, for a total of 128,094 samples collected. Fitting a Multinomial Naive Bayes Model, we find values for accuracy, precision, and recall in Table 3.7. In general, performance is lower than in Experiments 1 and 2 because of even length variations introduced by a larger set of candidates for other offices.

Candidate Combination Subsets. By viewing the TLS record lengths of different candidate combinations, we show that we can still compromise ballot secrecy (albeit to a limited extent)

Table 3.6: Proportion of Ballots by Possible Candidate Combinations, Experiment 2 (Cumulative).

		Possible candidate combinations											
		1	2	3	4	5	6	7	8	9	10	11	12
Proportion		8%	11%	14%	19%	22%	25%	37%	43%	69%	90%	100%	100%

for all ballots in a manner similar to Experiment 2. Of the 126 possible candidate combinations (tickets), we found:

- 1% of all ballots had a unique TLS record length for that candidate combination
- 12% of all ballots cast had TLS record lengths that were shared with 10 or fewer other candidate combinations
- 53% of all ballots cast had TLS record lengths that were shared with 73 or fewer other candidate combinations
- 100% of all ballots cast had TLS record lengths that were shared with 92 or fewer other candidate combinations. In other words, for all votes cast in this election, we know at least 33 different ways to mark a ballot that was not chosen by the voter.

Table 3.7: Performance on Test Set by Office, Experiment 3.

	Mayor			Councillor			Regional Councillor		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall	Accuracy	Precision	Recall
Bayes	33%	32%	33%	32%	33%	32%	63%	70%	63%
Guessing	17%	17%	17%	14%	14%	14%	33%	33%	33%

3.8 Mitigations

3.8.1 Client-Side Confirmation Page Generation

Transmitting the confirmation page over the internet can be avoided by generating the confirmation page on the client side in JavaScript. We observed the SwissPost and Neuvote systems taking this approach, rendering this particular side-channel *not-applicable*.

We met separately with representatives from Neuvote and Swiss Post and were granted private access to their (respective) demo systems. In both cases, we performed a basic analysis

by casting ballots and observing the responses in Charles (an HTTP proxy) and Wireshark. We observed no ballot-related network activity in the time between selecting a candidate and rendering the confirmation page, indicating the page is generated on the client side. We additionally observed that the cast ballot selections were encrypted at the application layer before being transmitted to the server. As expected, our experimental observations of packet lengths in Wireshark showed no perceptible correlation between candidate name length and network response length.

3.8.2 Fixed-Length Responses

Much discussion exists on the mitigation of length-based fingerprinting attacks, including adding padding to ensure the response is always of a fixed length. Gellert et al. describe such a scheme as “perfect length-hiding padding”, but also outline major performance tradeoffs [30].

We discussed this option with Simply Voting, but the practical limitations quickly became apparent. First, the padded size would need to be larger than the largest naturally-occurring response. The second is that the gzipped length is non-linearly dependent on the content itself, requiring the padding to either be calculated and applied *after* compression or for compression to be disabled.

Padding applied dynamically as a server header after compression is an atypical use case and would likely be difficult using standard server software. Disabling compression would needlessly slow page load times, which is highly problematic for an application involving large numbers of users making requests in a short window (i.e., election night). By default, many servers only compress MIME text/HTML. One solution might be to display candidate names as fixed-length images, although this would not, on its own, rule out the possibility it could lead to other distinguishing events.

3.8.3 Uniformly Random-Length Padding in Response Header

Coordinated disclosure with Simply Voting. Once we had confirmed our hypothesis with the results of Experiment 1, we contacted Simply Voting to make the coordinated disclosure. They acknowledged our result, which we discussed in-depth in a meeting. Overall, we found the interaction positive and constructive and commend them for their commitment to the disclosure process.

Following internal discussions with the engineers, they eventually settled on a mitigation involving adding a random amount of padding bytes sampled uniformly in the interval $[0, 1000)$. The sever added this padding in a new `X-Ballot-Secrecy` response header, which is now live

on their ballot confirmation pages.

Analysis of Simply Voting’s Fix. We implemented Simply Voting’s mitigation on our cloned server. We then re-ran Experiment 1 (see Section 3.6), which had 4 ballot options. With this mitigation enabled, our prediction strategy now had an accuracy of approximately 25%—reduced to (nearly) random guessing.

However, candidates with longer names become disproportionately distinguishable in instances where the X-Ballot-Secrecy header sampled close to the maximal length. For example, when a voter casts a ballot for Linda Marlene Eales (the choice that produces the largest ballot selection), if the X-Ballot-Secrecy header is near maximal (e.g., 998, 999, or 1000 bytes), it will produce a total TLS record length that is impossible to achieve with any other candidate choice. In that case, a passive observer would be able to identify that this voter cast a ballot for Linda with a high degree of certainty.

This phenomenon also exists when the ballot secrecy header is very close to its minimal length (e.g., 0 bytes), and a voter chooses to abstain (the choice produces the shortest ballot).

To quantify this, we can perform a similar analysis to the one we did in Experiments 2 and 3; we view the maximum and minimum TLS record lengths produced by each ballot choice and identify where these distributions do not overlap. If we observe a record length outside of the distribution of one of the ballot choices, we can deduce the ballot was *not* cast for that candidate. We conducted 8,000 trials per candidate for a total sample size of 32,000. We found:

- 0.25% of all ballots had a unique TLS record length for the candidate choice
- 0.38% of all ballots had TLS record lengths that were shared with 2 or fewer other candidate choices
- 1.18% of all ballots had TLS record lengths that were shared with 3 or fewer other candidate choices
- 98.83% of all ballots had TLS record lengths within the distribution of all other candidate choices

Simply Voting’s mitigation substantially lowers the risk of the attack presented in this chapter. Although a practical fix under the circumstances, it still poses a risk to ballot secrecy for some voters in some cases. Client-side confirmation page generation, therefore, should remain the eventual goal.

3.8.4 Padding From a Gaussian Distribution

Degabriele [24] addresses the issue of overlapping uniform length distributions in the context of the CRIME/BREACH attack, where multiple observations of the same ciphertext with random padding by an attacker can be used to leak actual record lengths. The problem is similar to the limitations we identified with uniform padding in the ballot secrecy context: An attacker can observe the difference in the maximum and minimum of overlapping distributions. Degabriele proposes mitigating this by using a truncated Gaussian distribution, reducing the number of items at the tail end of the distribution. Future work should study the extent to which this approach reduces the number of clearly identifiable ballots.

3.8.5 Discussion and Conclusion

Using the network-observed TLS record length of the voter’s vote confirmation page, our model predicted the chosen candidate in a recent real-world mayoral contest with 83% accuracy relative to random guessing (which had 25% accuracy). In more complex ballots, our model still outperformed random guessing. However, for a large subset of ballots cast in an election, we could still obtain limited information in the form of certain combinations of candidates who were *not* voted for. Validation of our models shows this performance difference is unlikely to be explained by sampling variation.

Perhaps the biggest takeaway for us, however, was how difficult it was to obtain access to voter demos. If the security of a civic election is in the public interest, companies should not need long internal deliberations to respond to a request to see what a voter already sees. In this regard, we hope the industry will eventually follow Simply Voting’s example and offer demos *pro forma*.

Chapter 4

Second Study: A Standards-based Review of Online Voting in Ontario Municipalities

4.1 Introductory Remarks

In the previous chapter, we explored a specific vulnerability from a specific online voting vendor in-depth—from discovery to disclosure. This alone may not be representative of the overall situation in Ontario, where over two hundred municipalities offer online voting using six different vendors. Ontario’s adoption of e-voting represents one of the largest and most diverse deployments of e-voting worldwide.

In this chapter, we take a broad approach to consider Ontario’s use of online voting as a whole. Given the critical nature of elections, the stakes are high. A natural and necessary question has emerged: How well does this technology align with the principles of free and fair elections? How well do these deployments measure up to an objective democratic benchmark? What should that benchmark even be?

To evaluate Ontario’s practices, we could compare them to a standard. However, no provincial or federal-level standards exist for online elections in Ontario. Until a standard can be developed and adopted domestically, we turn to perhaps the most natural and immediate stand-in: The Council of Europe’s (CoE) standards for e-voting, which offers a set of broad-ranging and well-suited requirements and guidelines for online voting. We use this baseline to present the first standards-based analysis of online voting practices in Ontario.

Our results find the province is broadly *non-compliant*, with only 14% of the CoE’s 49 standards and 93 implementation guidelines categorized as fully met. We summarize these differences and identify areas for improvement in the hope of underscoring the need for domestic e-voting standards.

4.2 Background and Preliminaries

The *Council of Europe* is an international organization focusing on human rights, democratic governance, and the rule of law. Founded in 1949, it predates the European Union. The CoE articulates its core values by developing standards and monitoring how well those standards are applied among member states.¹ The CoE consists of 46 member states, including all 27 members of the European Union, amounting to a combined population of over 700 million citizens. On the topic of online voting, the Council of Europe takes the view that such systems must be “secure, reliable, efficient, technically robust, open to independent verification and easily accessible” to build public confidence, which is a “prerequisite for holding e-elections” [2].

4.2.1 Terminology

The Council of Europe’s Standards of E-Voting (SeV) fall across three main documents [3, 4, 5]. Although distinct from the CoE SeV, the US Voluntary Voting System Guidelines (VVSG) [7] provides a model for conceptualizing standards as a hierarchy of four successive components: principles, requirements, guidelines and test assertions. Requirements are derived from principles. Guidelines flow from requirements and so on. We use the following terminology in this analysis:

Principles. Principles articulate the highest-level priorities. The CoE articulates principles in Section 14 of the explanatory memorandum [3]. These principles are democratic in focus (universal suffrage, equal suffrage, free suffrage, etc.), as opposed to the VVSG’s principles, which are more engineering-focused (quality design, quality implementation, interoperability, etc.).

Requirements. Requirements are properties of the election that must be upheld. The CoE articulates its requirements in its main standards document [5]. For example, Requirement 10 (under the principle of free suffrage) requires a voter’s intention to be free of undue influence.

Guidelines. Guidelines provide some specificity around what is minimally necessary to meet a requirement. The CoE articulates guidelines for some (but not all) of its requirements [4]. For example, toward the requirement of freedom from undue influence, Guideline 10(d) advises that the voting system “offer mechanisms ... to protect voters from coercion to cast a vote in a specific way.”

¹<https://www.coe.int/en/web/portal/european-union>

Directives. For the sake of our analysis, we combine the concepts of requirements and guidelines into a single category: *directives*. In total, we examined 141 directives consisting of 49 requirements and 92 guidelines.

4.2.2 Information Collection About Ontario Municipal Online Voting Practices

We consulted various information sources to determine whether practices in Ontario complied with directives. We sampled public-facing election documents on municipal websites, read minutes from municipal council meetings, viewed advertised security claims by the five private online election vendors active in Ontario, used search engines to find news reports and press releases about technical incidents, and searched Twitter with incident-related keywords to identify incident response communications from municipalities and vendors. We collected tutorial videos created by municipalities for each vendor, and evaluated a public interactive demonstration system from one vendor as well as a private interactive demonstration system from another. On election day, we performed a passive security analysis of the voting portals of five municipalities, each using a different one of the five online voting vendors active in Ontario.

We indicated that **information was broadly unavailable** if, after a thorough search, no information about compliance with a directive was publicly available. For example, we are not aware of a single penetration test report being made public by any of Ontario’s 217 municipalities despite five years of research in this area: We are confident that the publication of these documents is, at the very least, extraordinarily rare.

Legal standing. Canada and the United States have observer status in the CoE. Although Canada is deeply aligned with the legal and ethical values of the CoE, as a non-member state, the SeV has no legal standing in Canada. Consequently, our findings of compliance (or, more importantly, *non-compliance*) are entirely moot from a legal perspective. As such, there is no explicit expectation that any of the directives be met—except where they overlap with the governing legislation (i.e., Ontario Municipal Elections Act [1]).

4.2.3 Related Work

Del Blanco et al. [25] and Luis Panizo et al. [8] performed a cryptographic analysis of the *nvotes* and Helios Voting e-voting systems, respectively, on the CoE’s requirements for e-voting. This research identified technical limitations concerning these systems’ coercion resistance and end-to-end verifiability, among other aspects. Our study diverges from previous

work because it not only analyzes the technology of e-voting systems but also the *real-world implementation* of these systems by municipal governments. Our analysis is broader in that it examines additional categories of CoE directives: namely those related to procurement, transparency, certification, regulation, reliability, and accountability.

4.2.4 Compliance Categories

We began the analysis by attempting to assign each directive to one of three broad compliance categories (*met*, *partially met*, *unmet*). As the analysis proceeded, we identified several additional cases and sub-cases. Each directive was eventually assigned one to one the following categories defined as follows:

1. **Directive broadly *met*** (●)

(a) Most (or all) cities meaningfully meet directive.

2. **Directive *partially met*** (◐)

(a) Some cities fully meet directive.

(b) A substantial number of cities meaningfully attempt to meet directive.

3. **Directive broadly *unmet*** (○)

(a) Few cities meaningfully attempt to meet directive.

(b) Almost all (or all) cities fail to meaningfully attempt to meet directive.

(c) No cities (to our knowledge) meaningfully attempt to meet directive.

(d) General failure of provincial jurisdiction.

4. **Information broadly unavailable** (⊗)

(a) The required information to assess is generally not publicly available.

5. **Not applicable** (⊙)

(a) Assessing the directive is outside authors' recognized area of expertise.

(b) Directive does not apply to the Ontario legal/electoral case.

(c) Directive does not apply to the online voting setting.

Principle	Met	Partial	Unmet	No Info	N/A
Accountability	1	9	3	-	-
Equal Suffrage	3	4	-	1	2
Free Suffrage	3	2	7	2	2
Regulatory & Organisational	3	2	16	5	1
Reliability and Security	1	6	8	17	1
Secret Suffrage	4	2	8	2	1
Transparency and Observation	3	1	10	1	1
Universal Suffrage	1	-	-	1	7
Total	18	18	58	32	15
Proportion (Applicable)	14%	14%	46%	25%	-

Table 4.1: Summary of compliance

4.3 Summary of Findings

Our analysis shows that Ontario municipalities are broadly non-compliant with the CoE’s directives. A summary of our analysis is shown in Table 4.1. A substantial effort has only been made to satisfy 28% of applicable directives, and half of those (14%) are only partially met. One in four directives could not be evaluated because of a lack of transparency by vendors and municipalities.

When viewing directives by category, we identify three key trends. First, the majority of directives relating to Regulatory & Organizational Requirements are unmet because Ontario has no standards for e-voting. Second, a disproportionate number of directives within the Reliability and Security category could not be evaluated, because both municipalities and vendors do not disclose information about voting system internals and procedures. Finally, two-thirds of the applicable directives in Transparency and Observation were unmet, which is indicative of the lack of transparency in municipal e-voting in Ontario.

4.4 Analysis of Selected Directives

The Council of Europe’s standards for e-voting consist of 141 directives for electoral authorities, legislators, and vendors. Our categorization for each directive is available in Section 4.6. In this section, we provide a selection of our more interesting findings, with the titles of directives paraphrased and shortened.

4.4.1 Directive Broadly Met

SeV §4. Election must be obviously real

Voters receive official notification by mail of an election, indicating that the election is real. From work done in Study 1, it is apparent demonstration/test systems are generally unavailable, so voters are unlikely to be confused.

SeV §5. Voting information (e.g. list of candidates) should not be presented differently on different channels

A legal principle of the Municipal Elections Act is that “voters and candidates shall be treated fairly and consistently” [37]. Specifically, Section 41(2) of the Municipal Elections Act (MEA) specifically outlines how candidates appear on the ballot [1]. Our observations show that cities present information about candidates neutrally and consistently, with no additional information about candidates on the online or in-person ballots, which satisfies implementation guidelines 5(a) and 5(b).

SeV §12. Voters should not be rushed and should have confirmation

To the best of our knowledge, all online voting systems in Ontario offer confirmation pages and do not rush voters. Study 1 tested the confirmation pages of Scytl, Simply Voting and Neuvote and found the confirmation pages allow voters to alter their choice, which satisfies implementation guideline 12(a).

SeV §22. Voter list should only be accessible to authorised parties

We interpret this to mean voter lists. Unlike American states like Ohio,² voter lists are not made publicly available and are only accessible to authorized parties (candidates, municipalities, and other election-related authorities).

SeV §32. Voters should be provided information about online election

Almost all, if not all, cities provide detailed information about e-voting, including technical support and documentation (satisfying 32(a)). Common methods of outreach include direct mail, city websites (although we observed many cities had outages of their websites on election night), videos posted to YouTube, and Tweets (satisfying 32(b)).

²<https://www6.ohiosos.gov/ords/f?p=VOTERFTP:STWD:::stwdVtrFiles>

SeV §45. No release of information about votes and voters before counting commences

We did not see election results released prematurely in any municipality, other than turnout data [38].

4.4.2 Directive Fully Met by Some Cities**SeV §9. Count one vote per voter**

There were several examples of voters receiving multiple voting credentials,³ which could allow them to vote twice. This is due to duplicate entries on the municipal voters list, or entries for deceased voters not being removed. The severity of this issue varies by municipality, as some have more robust processes in place to identify and remove duplicates.

SeV §10(b). Only official information on e-ballot

Two online voting vendors did not have HTTP Strict Transport Security (HSTS) preloading configured, which could allow for a Machine-in-the-Middle (MITM) [13]. Additionally, these vendors did not set `X-Frame-Options` header. Combined, this allows for a MITM to add unofficial information to an embedded version of the e-ballot. This vulnerability will be reported in detail in future work.

SeV §15. Individual verifiability

Individual verifiability exists for some cities using Scytl or Neuvote, including Markham [14] and Ignace [39], respectively. While there are limitations to these approaches (closed-source verifier app), the directive is met. Scytl's individual verifiability comes at the expense of SeV Requirement 23, because it shows who you voted for and could be used to prove to others how you voted [14]. However, most cities in Ontario use unverifiable voting systems offered by Dominion, Simply Voting, and Intelivote.

SeV §23(b). No residual information about voter's choice after voting

Simply Voting's unverifiable voting service purges information about the voter's choice from the browser cache. However, the proofs offered by municipalities using Scytl's individually verifiable voting violate this directive [14].

³<https://www.thorold.ca/en/news/thorold-residents-encouraged-to-hold-on-to-all-voter-letters-they-receive.aspx>

SeV §25. Previous choices (deleted) by the voter in the voting process should also be secret

Ontario does not allow for multiple votes to be cast as a feature against coercion resistance, so this directive was interpreted to refer to the secrecy of a voter's potential choice (before they confirm their choice). For most online voting vendors we had demo access to, confirmation pages were generated on a client-side basis, so deleted choices are kept secret. Study 1 showed that in the case of Simply Voting municipalities, a voter's potential choice is sent to the server, and the server generates a confirmation page. The vote is only protected in transit and can be read by the server. This practice could jeopardize the secrecy of both a voter's unconfirmed choices and their final vote.

SeV §29(a). Transparent procurement

Procurement rules vary by municipality, but generally, in Ontario, the purchase of online voting technology is not distinct from any other purchase of goods. Smaller contracts of under \$25,000 are generally partially exempt from procurement transparency/competitiveness requirements. In some municipalities, contracts below \$10,000 do not require a competitive process at all. For example, in 2022 Township of Central Huron had 6863 electors.⁴ In 2018, they entered a contract with Simply Voting at the cost of \$1.30 per elector [43], which is well below their threshold of \$25,000 for a competitive public procurement process [44].

SeV §32(c). Public demo of e-voting system

Study 1 showed that most vendors do not offer public demos of their e-voting systems.

SeV §40(a). No downtime

Municipalities using Dominion as a vendor experienced service disruptions in 2018 [12] and in 2022.⁵⁶⁷

SeV §40(i). Disaster recovery plans should exist

Before 2018, cities generally did not have disaster recovery plans [12] Because of outages in 2018 that led to emergency extensions of voting periods, disaster recovery plans were created by some affected municipalities. These plans are generally not available to the public.

⁴<https://www.centralhuron.ca/en/your-municipal-government/2022-official-municipal-school-board-election-results.aspx>

⁵<https://twitter.com/NewTecumseth/status/1584694858471690240>

⁶<https://twitter.com/TwpofScugog/status/1584689666259030016>

⁷https://www.thecounty.ca/county_news_notices/online-voting-extended-until-830-pm-on-october-24/

4.4.3 Directive Partially Met by Most or All Cities

SeV §9(c). Generally, voters should be prevented from casting multiple votes

Cities often use electronic poll books to prevent cross-channel multiple voting. However, the recurring issue of duplicate entries on the voters' list could allow voters to vote twice online.

SeV §39. Open and comprehensive auditing, with active reporting on issues/threats

Most voting vendors offer some form of logging, intrusion detection systems, and/or auditing features, but these audit systems are not comprehensive to the extent described in the explanatory memorandum [3]. For example, most municipalities do not offer individual or universal verifiability, so audit systems generally cannot provide proof of the authenticity of votes.

4.4.4 Directive Unmet: Meaningful Attempts From Some Cities

SeV §10. Voting system must be protected from MITM, client-side malware, etc.

Our analysis of the security posture of online voting services showed that Simply Voting is the only vendor with effective protection (HSTS pre-loading) against Machine-in-the-Middle attacks. Individual verifiability can protect against client-side malware but is only offered by cities using Neuvote/Scytl/Voatz. Cities using Intelivote/Dominion have neither of these features.

SeV §24. Disclosure of premature results should be prevented by system

Study 1 showed that for Simply Voting and Dominion's online voting services, the encryption of ballots occurs only in transit between the voter's device and the server (TLS), which means that the online voting provider has real-time access to and could prematurely disclose the count of votes for a candidate. By comparison, with cryptographically verifiable voting systems like the SwissPost e-voting system, the results stay encrypted until after the voting period. From observing their demonstration system, Scytl may offer some form of cryptographic protection against the release of premature results. Information is not available about the protections in place for other vendors.

SeV §42(a). Equipment should be checked and approved by a municipality-defined protocol before each election

Some municipalities conduct penetration tests against online voting systems on an informal and irregular basis. However, to the extent of our knowledge, no municipalities check/approve

equipment used by the vendor before each election.

4.4.5 Directive Unmet by Almost All Cities

SeV §10(a). Voter should be told how to verify connection to server

This directive is challenging to satisfy because there is no single voting portal in Ontario. The URL for online voting varies by vendor, and sometimes the URL varies between different elections. Few Ontario municipalities offer meaningful instructions to verify connections and protect against phishing. An example of ineffective instructions is the municipality of Clarington, which has a document titled “How can I verify I am accessing the actual voting site and not a fake site?” with the instructions “When accessing the voting website, HTTPS and an image of a padlock will appear in the search bar, confirming a secure connection”.⁸ These instructions are potentially dangerous, because phishing sites often use HTTPS, and no instructions are provided to check that the URL in the address bar exactly matches the official URL of the voting website.

SeV §10(d). Coercion resistance

The Municipal Elections Act does not specifically address the possibility of coercion in unsupervised remote voting. While it is an offence under the Act to coerce a voter, there are no legislated means to enforce or protect against this. Some cities offer supervised remote voting, where coercion could be difficult. This is offered for accessibility purposes; there are few in-person locations in a municipality, and a coercer could direct you to vote remotely instead.

SeV §11. Procedural steps ensure e-voting ballot is authentic

We are aware of informal logic and accuracy testing conducted by scrutineers and clerks, which may detect errors. However, these procedural steps are not required by law, and details of informal procedures are not made public. An example of non-binding, unclear procedures is “...the Clerk can test the system by running a mock election, and may investigate the feasibility of including candidates and scrutineers in this process...” [42]. Two cities had serious errors which could have been prevented by sufficient procedural steps. Thunder Bay had some voters receive the wrong ballot [54], while Cambridge presented an e-ballot to voters that was missing candidates [40].

⁸<https://votes.clarington.net/en/voters/voter-faqs/>

SeV §19. Ballot secrecy

For most cities, the e-voting system can see a voter's date of birth and the city a voter is voting in. If combined with that city's voter list, many voters can be re-identified merely with their birthday [12].

SeV §27. Gradual introduction to e-voting

Adoption of online voting in Ontario has been rapid—doubling each election cycle between 2003 to 2018. Cities do not generally run pilot projects (fails Directives 27(b), 27(d)), and while some cities conduct feasibility studies, they are often not available to the public. Three examples of sudden adoption with no hybrid voting include Adjala-Tosorontio, which transitioned from exclusive in-person paper ballots in 2018 to exclusive remote e-voting in 2022, Algonquin Highlands, which transitioned from exclusive mail-in voting in 2018 to exclusive remote e-voting in 2022, and Arran Elderslie, which transitioned from exclusive mail-in voting in 2018 to exclusive remote e-voting in 2022.⁹¹⁰

4.4.6 Directive Unmet by All Cities**SeV §17, 19, 10(c). Directives that require universal verifiability**

No cities in Ontario offered universal verifiability where any interested person could verify that votes are counted correctly.

SeV §21. Authentication data should be protected

Voter dates of birth are used for authentication, which cannot be meaningfully protected. As well, credentials delivered by mail are sometimes visible through envelopes when held up to light [12].

SeV §23. Proofs of who a voter voted for can't be used by third parties

The verification method employed by ScytI shows the voter which choice they selected [14]. Any third party, given a QR code and a voter's credentials, could verify this proof themselves. Most other vendors offer no proof.

⁹Vote methods in 2018: <https://whisperlab.org/ontario-online.csv>

¹⁰Vote methods in 2022: <https://elections2022.amo.on.ca/web/en/home>

SeV §23(c). Voters should be informed of risks to ballot secrecy and mitigations

We did not find evidence of cities informing voters of risks to ballot secrecy. Instead, several municipalities in 2022 repeated vendor claims of perfect secrecy on social and traditional media.¹¹¹² This claim appears to originate from a 2018 document provided by Simply Voting to municipalities:

Whether you use the internet or telephone to vote, your vote is instantly encrypted and stored with no possibility of your vote being traced back to your identity, just like a traditional paper ballot. It is impossible for municipal staff, Simply Voting employees or any other person to see how you have voted [6].

However, a recent analysis of Simply Voting's demonstration system shows that no application-layer cryptographic mechanism separates a voter's choice from authentication data like their birthday before a vote is cast. Another study found over 50% of Ontario voters are uniquely re-identifiable from their city and date of birth [12].

SeV §29. Legislation to regulate e-voting systems should ensure an electoral management body has control over them

E-voting systems are broadly unregulated: Vendors have control over e-voting systems and are entirely responsible for deploying and managing remote e-voting infrastructure (fails to satisfy 29(d)).

SeV §30. Observability and responsibility of count

The vendor is responsible for the counting process, not an electoral management body. In addition, the widespread absence of satisfactory universal verifiability means the evidence of correct counting is not sound (fails to satisfy 30(b) and 30(c)).

SeV §31, 31(a-b), 33, 33(a-f), 34. Transparency, disclosure, and observation

Private vendors are not subject to access-to-information law, have little transparency, and use proprietary systems. Testing of e-voting systems is conducted privately. Observers are not able to access meaningful documentation on e-voting systems, inspect physical/electronic safety mechanisms, or inspect or test devices.

¹¹<https://twitter.com/ClaringtonON/status/1555184785089347596>

¹²<https://www.baytoday.ca/2022-municipal-election-news/election-officials-easing-concerns-about-online-voting-system-5944887>

SeV §36, 36(a), 37, 37(a-f), 38, 40, 43. Directives relating to certification requirements or standards

No certification requirements or standards exist in Ontario.

SeV §41. Only people authorized by municipality can have access to infrastructure

Private vendors are wholly responsible for managing remote e-voting infrastructure. They, not municipalities, are responsible for authorizing their staff members according to their policies.

4.4.7 Directive Unmet Due to Failure Within Provincial Jurisdiction**SeV §28, 28(a-f). Legislative directives for remote e-voting**

The Municipal Elections Act is limited, delegating responsibility for authorization of “alternative voting methods” to cities, which can pass bylaws to authorize online voting. These bylaws are extremely limited in scope; Below is Markham’s entire bylaw to authorize online voting:

That the use of internet voting is hereby authorized for the purposes of voting in municipal elections in the City of Markham [15].

Neither provincial law nor municipal bylaws have procedures for e-voting implementation, set-up, operation, or counting. They do not specify how to determine e-vote validity, have rules for problems/failures/discrepancies for verification tools, or specify timelines for e-voting. Although some data destruction is required by law, it is described in the context of paper elections, and procedures for digital data destruction are not legislated [1]. Provisions exist for candidates or municipalities to appoint observers, but these provisions appear to be written in the context of paper elections: no provisions define roles or access provided to observers in online elections. Municipal clerks (executive, not legislative) are responsible for determining procedures for e-elections.

4.4.8 Not Applicable

We determined that some directives were not applicable because they were outside of our expertise, not relevant in the Ontario municipal elections context, or focused on technology other than online voting.

Directives 1, 1(a), 1(c), 2, 2(a), 2(b), 3, 40(f) require a usability background to properly evaluate. These are outside of our expertise.

We are not aware of municipalities that have coercion-resistant multiple voting and voters are not allowed to cast votes over multiple channels, so 9(a) and 9(b) do not apply in the Ontario context. 28(i) is also not applicable because Ontario municipalities have a grace period for in-person and online voting. This allows voters to submit their ballot after voting has ended, provided that they have begun the voting process before the end of the voting period.

15(a), 15(b), and 23(a) refer specifically to the use of e-voting machines in supervised environments. These are not applicable to our study of remote e-voting systems in Ontario.

4.4.9 Information Not Available

We were unable to evaluate many directives because of a lack of transparency from vendors and municipalities. We encountered issues in four areas:

Directives Requiring Access to ‘Live’ Election Systems

Our access was limited to the login page of each vendor as well as demonstration systems offered by two vendors using mock elections. For that reason, we were not able to evaluate whether voters could cast an abstain vote (13) or whether they are advised of invalid votes (14), among other directives.

Directives Requiring Knowledge of Vendor Procedures

Vendors are not subject to access-to-information law and do not disclose details of their procedures to the public. For that reason, we were not able to evaluate which auditing directives vendors satisfied (39(a,b)) or whether e-voting infrastructure is properly secured (40(d)), among other directives.

Directives Requiring Knowledge of Online Voting System Internals

Online voting products made by private vendors are proprietary and not subject to access-to-information law. Source code, configuration, and technical documentation are not available to the public. For that reason, we were unable to evaluate how voter information is separated from their decision (26(a)) or whether irregular votes can be identified by the system (49), among other directives.

Directives Requiring Knowledge of Municipal Procedures

Municipalities generally do not disclose their internal procedures for conducting elections besides the few documents they must make publicly available (e.g. mandatory accessibility re-

ports). For that reason, we were unable to evaluate whether the two-person rule is followed when sensitive data is accessed 41(b,c), whether the authenticity and integrity of voter lists are confirmed (48), or whether online and non-online votes are aggregated securely (6), among other directives.

4.5 Recommendations and Conclusion

With only 18 of 126 (14%) of applicable directives in the Council of Europe's Standard for E-Voting fully met, Ontario and its 217 municipalities engaging in online voting have much to do. We conclude with five key recommendations:

Recommendation 1. Cities should be familiar with international democratic principles, expectations and norms.

There is a valid role for criticism of online voting in the province, especially if the technology diverges from internationally accepted democratic norms. Toward understanding which forms of criticisms of online voting are (and are not) justified or warranted, cities ought to, at a minimum, become acquainted with the CoE's Standards for E-Voting.

Recommendation 2. Cities should conduct their own internal review.

Cities should conduct an internal review of their compliance relative to the SeV. This could help cities identify areas of risk and improvement.

Recommendation 3. Province should update the Municipal Elections Act.

16 unmet directives directly pertain to the province's lack of a legislative framework for e-voting. Numerous others exist indirectly as a consequence.

Recommendation 4. Make information about e-voting policies, procedures and protections more widely available.

The SEV is clear: Information on the functioning of an e-voting system shall be made publicly available [2]. We could not assess 32 directives because necessary information was unavailable.

Recommendation 5. Make election results evidence-based.

As the CoE explains, independent verification is needed to build public confidence, which is a "prerequisite for holding e-elections" [2]. Independent verification such as cryptographic

end-to-end verification (E2E-V) would address many unmet directives.

4.6 Summary of Analysis

This section contains a list of all directives contained within the Council of Europe Standards for E-Voting with titles paraphrased and shortened. Our evaluation (if applicable) for each directive is also given.

#	Paraphrasing	Score	#	Paraphrasing	Score
1	UI should be easy to use	⊙ ^a	19(a)	Voter list separated from voting components	●
1(a)	Easy to interpret voting options	⊙ ^a	20	Data minimization	⊗
1(b)	Voters involved in design	⊗	21	Authentication data is protected	○ ^f
1(c)	System compatibility	⊙ ^a	21(a)	Authentication uses cryptography	○ ^d
2	Independence for disabled voters	⊙ ^a	22	Voter list has access control	●
2(a)	Special voting interfaces	⊙ ^a	23	No transferable proof of cast vote	○ ^f
2(b)	WCAG 2.0 AA compliance	⊙ ^a	23(a)	Paper-based proofs	⊙ ^c
3	Other voting channels available if e-voting not universally accessible	⊙ ^a	23(b)	No residual info after casting	● ^h
4	Live election interface is explicit	●	23(c)	Voters informed of ballot secrecy risks and mitigations	○ ^f
5	Voting info presented uniformly	●	23(d)	Voters taught to remove traces from devices	○ ^e
5(a)	No superfluous info on ballot	●	24	No disclosure of premature results	○ ^d
5(b)	No biased info about candidates	●	25	Pre-cast selections also secret	● ^h
6	Secure aggregation across channels	⊗	26	Voters anonymous during count	○ ^e
7	Voters uniquely identifiable	● ⁱ	26(a)	Voter identity and choice separated	⊗
8	Voters authenticated	● ⁱ	26(b)	Ballots decoded ASAP after close	●
9	One vote per voter...	● ^h	26(c)	Confidentiality during auditing	●
9(a)	...even if multiple casts allowed	⊙ ^b	27	Gradual introduction of e-voting	○ ^e
9(b)	...even if multiple channels	⊙ ^b	27(a)	Public feasibility study beforehand	○ ^e
9(c)	Multiple casts prevented otherwise	● ⁱ	27(b)	Early pilots	○ ^e
10	Voting system is protected	○ ^d	27(c)	Final system tested before election	⊗
10(a)	Voter taught to verify connection	○ ^e	27(d)	Comprehensive pilots	○ ^e
10(b)	Only official information on ballot	● ^h	28	Legislation enacted beforehand	○ ^g
10(c)	Cast ballots are tamper-resistant	○ ^f	28(a)	Law: Implement/operate/count	○ ^g
10(d)	Coercion resistance	○ ^e	28(b)	Law: Vote validity	○ ^g
11	Procedures ensure authentic ballot	○ ^e	28(c)	Law: Discrepancies in verification	○ ^g
12	Proper voter intent-capture	●	28(d)	Law: Data destruction	○ ^g
12(a)	Ballot modifiable before casting	●	28(e)	Law: Domestic/int'l observers	○ ^g
13	Voters can cast an abstain vote	⊗	28(f)	Law: Timelines	○ ^g
14	Voters are advised of invalid votes	⊗	28(g)	No voting before voting period	●
15	Individual verifiability	● ^h	28(h)	E-voting before in-person allowed	●
15(a)	Paper copies of votes at polls	⊙ ^c	28(i)	No voting after voting period	⊙ ^b
15(b)	Statistical audits (e.g. RLAs)	⊙ ^c	28(j)	System delays don't invalidate vote	⊗
16	Confirm of cast ballot	●	28(k)	System inaccessible after election	●
17	Can verify <i>all</i> valid votes incl.	○ ^f	29	EMB has control over system	○ ^f
18	Can verify <i>only</i> valid votes incl.	○ ^f	29(a)	Transparent procurement	● ^h
19	Ballot secrecy	○ ^e		<i>Continued on next page...</i>	

●: Fully met ●: Partially met ○: Not met ⊗: Info not available ⊙: Not applicable

^a Not evaluated (outside expertise)

^b Not applicable to Ontario case

^c Not applicable to online voting

^d Some meaningfully attempt

^e Almost all cities failing

^f No cities attempt

^g Provincial failure

^h Some cities fully meet

ⁱ Nearly all cities attempt

#	Paraphrasing	Score	#	Paraphrasing	Score
...Continued from previous page			40(b)	Inform voters of incidents	● ^h
29(b)	Limit conflicts of interest	● ^h	40(c)	No eligible voters excluded	● ^h
29(c)	Separation of duties	⊗	40(d)	Cast votes are accessible, secure, and accurate	⊗
29(d)	Not unduly dependent on vendor	○ ^f	40(e)	No data loss when technical problems occur	⊗
30	Observability of the count	○ ^f	40(f)	Security mechanisms consider usability	○ ^a
30(a)	Records of vote-counting process	⊗	40(g)	System uptime regularly checked	⊗
30(b)	Evidence-based vote counts	○ ^f	40(h)	E-voting infrastructure is secure	⊗
30(c)	Accuracy features are verifiable	○ ^f	40(i)	Disaster recovery plans exist	● ^h
30(d)	Availability/integrity of ballot box	⊗	40(j)	Possible to check state of protection of voting equipment	⊗
31	Transparency	○ ^f	40(k)	Permanent backup plans available	⊗
31(a)	Published list of software used	○ ^f	40(l)	Incident response protocols available to staff	⊗
31(b)	Public access to source code, docs	○ ^f	40(m)	Post-election securely stored	⊗
32	Voters provided info about election	●	41	Only authorized people have access to infrastructure	○ ^f
32(a)	Docs and support how to vote	●	41(a)	System access limited to necessary function	⊗
32(b)	Voter info widely available	●	41(b)	Two-person rule, mandatory reporting and monitoring during voting	⊗
32(c)	Public demo of e-voting system	● ^h	41(c)	Two-person rule for other critical technical activity	⊗
33	Disclosure of system components	○ ^f	42	Deployed voting system is genuine and operates correctly	○ ^f
33(a)	Detailed/reliable observation data	○ ^f	42(a)	Equipment checked before each election	○ ^d
33(b)	Observers have access to docs	○ ^f	43	Software updates are re-certified	○ ^f
33(c)	Docs in common language	○ ^b	43(a)	Infrastructure deployment procedures	⊗
33(d)	Observers trained by cities	⊗	44	Vote immutable once cast	● ^h
33(e)	Observable hardware and software testing	○ ^f	45	No info released about votes and voters before counting commences	●
33(f)	Observable certification process	○ ^f	46	Secure handling of cryptographic material by electoral body	○ ^e
34	Observable election	○ ^f	46(a)	Cryptographic key generation ceremony open to public	○ ^f
35	Component interoperability	○ ^f	47	Integrity incidents are reported	⊗
36	Standards must exist for e-voting	○ ^f	47(a)	Integrity threats specified in advance	○ ^e
36(a)	Certification aims and methods 36	○ ^f	47(b)	Incident mitigations specified	● ^h
37	Independent review of compliance	○ ^f	48	Integrity of voter/candidate lists	⊗
37(a)	Certification costs determined	○ ^f	48(a)	Security of printing process for voter cards	⊗
37(b)	Certification bodies receive relevant info and get sufficient time	○ ^f	49	System identifies irregular votes	⊗
37(c)	Certification mandate regularly reviewed	○ ^f	49(a)	System determine if votes cast within time limit	⊗
37(e)	Certification reports are self-explanatory	○ ^f			
37(f)	Disclosure of certification docs	○ ^f			
38	Certified system is immutable	○ ^f			
39	Open and comprehensive auditing	● ⁱ			
39(a)	Detailed auditing requirements	⊗			
39(b)	Components have synchronized time sources	⊗			
39(c)	Audit conclusions considered in future elections	⊗			
40	Municipality is responsible for compliance, availability, reliability, usability, and security.	○ ^f			
40(a)	No downtime	● ^h			

●: Fully met ●: Partially met ○: Not met ⊗: Info not available ○: Not applicable

^a Not evaluated (outside expertise)

^d Some meaningfully attempt

^s Provincial failure

^b Not applicable to Ontario case

^e Almost all cities failing

^h Some cities fully meet

^c Not applicable to online voting

^f No cities attempt

ⁱ Nearly all cities attempt

Chapter 5

Discussion, Future Work, and Conclusion

5.1 Discussion

5.1.1 Central Role of Private Sector

Both the Council of Europe’s Standards for E-Voting and the Swiss Ordinance on Electronic Voting (OEV) place clear restrictions on the role of the private sector. The former says clearly that “legislation shall. . . .ensure that the electoral management body has control over them [e-voting systems]” while the latter has several restrictions on the role of the private system operators. In Ontario municipalities, however, the private sector plays a central role in the on-line voting context. Private vendors are typically responsible for operating all components of the e-voting system and printing and mailing credentials to voters. This, in turn, raises several concerns. The Municipal Freedom of Information and Privacy Act, which allows interested individuals to request documents from municipalities, does not apply to these private vendors, which severely restricts the ability of journalists or residents to obtain election-related information in contests using online voting. Additionally, the interests of these vendors may not align with the public interest.

5.1.2 Implications of Vulnerabilities

Security vulnerabilities can weaken public confidence in e-voting. The findings of Study 1 are being used by some residents of South Bruce, Ontario, to request that a local referendum on a proposed nuclear waste facility be conducted via paper ballot, instead of using e-voting [11].

It is important to note that the vulnerabilities and weaknesses described in both studies were discovered in production online voting systems being used in Ontario municipal elections. As noted in Study 2, these systems were deployed without a robust public testing period or

pilot projects, making vulnerabilities both more difficult to discover and the impacts of these vulnerabilities more severe. This differs greatly from other jurisdictions where public testing and pilot projects are required by law.

5.1.3 Challenges in Mitigation

Even when vulnerabilities in online voting systems used in Ontario are discovered by security researchers, major barriers to mitigation exist. Study 1 showed that half of vendors did not respond to requests relating to the discovery of a severe ballot secrecy vulnerability. The Swiss OEV requires election administrators to have a process for handling reported flaws which ensures that “all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users.”

5.2 Future Work

5.2.1 Domestic Standards Development

The Digital Governance Standards Institute (DGSI) is currently developing Canadian standards for online voting in consultation with academics, industry, and municipal officials. This standard is in development: the DGSI recently held a public review in late 2023/early 2024¹.

While it is promising that a standard for e-voting is in development in Ontario, there are some limitations to this process. Because this standard is developed in consultation with private online voting vendors, some requirements of other international standards (for example, the Swiss prohibition of outsourcing some components to the private sector) are unlikely to be included, regardless of their merit. Another limitation is the voluntary nature of the standard: Online voting vendors and municipalities may or may not comply. This stands in contrast to the Swiss Ordinance on Electronic Voting, which is legally binding. Even the Council of Europe’s Standards for E-Voting (CoE SeV), which are not automatically binding, have been adopted by several member states and referred to in a Supreme Court ruling in Estonia [46].

Despite these limitations, a completed DGSI standard does present an exciting opportunity for future work. The standards-based analysis performed in Study 2 could be repeated with the DGSI standard instead of the CoE SeV, or the DGSI could be compared to the CoE SeV. This would provide the public, policy-makers, and academics with helpful information to judge the effectiveness and adoption of this new pan-Canadian standard.

¹<https://dgc-cgn.org/can-dgsi-111-public-review-for-online-voting-standard-now-open/>

5.2.2 Research in the 2026 Municipal Election

Performing another standards-based review of Ontario’s online municipal elections during the 2026 election cycle with the CoE SeV would allow us to track whether practices in Ontario are improving or degrading relative to 2022. It would also allow researchers to determine specifically what categories are seeing the most and the least improvement, and provide some insight into whether the proposed DGSi online voting standards have caused practices to noticeably change in Ontario.

Additionally, this research could be expanded to provide individual standards-based reviews of individual municipalities. While it is likely infeasible to review the hundreds of municipalities in Ontario conducting elections online, it may be possible to choose several major municipalities and compare their policies and practices using the CoE SeV or DGSi standard as an objective benchmark. This is a valuable opportunity to identify areas where all municipalities are succeeding or failing, and where individual cities differ in terms of their practices.

5.2.3 Public Access and Testing

In Switzerland, major issues were discovered (and fixed) in the online voting system’s universal verifiability through a public testing phase, where security researchers were invited to find vulnerabilities [23]. Providing public access to source code and a robust public testing period in Ontario may help build public confidence in online voting technology and ensure that vulnerabilities are discovered before elections occur.

In Switzerland, these practices are required by law. The provincial government of Ontario could update the Municipal Elections Act to require these practices. Municipalities could also work with vendors to create opportunities for public testing and review of these systems.

5.2.4 Alternatives to PIN and Date of Birth Authentication

Estonian voters use their government-issued ID cards to authenticate for e-voting. Voters use a smart card reader to connect their ID card to their computer. When they provide their card PIN it authorizes the voter and signs them into the e-voting system [41].

The Estonian scheme has advantages when compared to authentication schemes in Ontario municipal elections. Unlike Ontario, Estonian voters do not receive voting credentials in the mail, so it is not possible for these to be intercepted or for these credentials to go to past addresses of a voter. Additionally, a user-chosen PIN is generally considered more secure than a user’s birthday.

5.2.5 National Public Certification and Ownership

It's important to consider whether the current privatized model of running online elections is ideal, and if better alternatives are possible.

Instead of each online-voting municipality in Ontario individually determining their cybersecurity requirements for their elections, a simple improvement could be for the federal government to create a certification body that can identify which online voting vendors meet key cybersecurity requirements. This can better inform municipalities on which private vendors they should do business with.

It may be better yet to fundamentally change the model of online voting in Canada to a publicly administered one. Like in Switzerland, Canada's federal government could be tasked with developing a source-available online voting solution. This entity could be given a mandate to offer election services to municipalities in Canada. This fully public model offers several advantages. First, transparency would be improved, as access-to-information law would apply to the online voting vendor. Second, a public model removes the profit motive, which could allow for the public online voting vendor to service smaller clients with an otherwise unprofitable amount of service and technical support. Finally, it allows for infrastructure to be managed directly by the federal government with the advice and protection of Communications Security Establishment (CSE), Canada's national cryptologic agency.

5.3 Conclusion

The work done in Studies 1 and 2 clearly shows that much needs to be done to ensure that municipal elections conducted in Ontario meet basic democratic principles of transparency, accountability, and verifiability.

Study 1 showed that a major ballot secrecy vulnerability existed in an online voting vendor in Ontario. Moreover, the nature of such an issue was quite simple—inferring user behaviour from length-based analysis of ciphertext is hardly novel, even in the online voting context. It raises the important question of whether, in the absence of standards, security oversights like this are bound to happen. The lack of cooperation from other vendors that may have been vulnerable raises further concerns for transparency and accountability.

Study 2 does much to answer these questions and address these concerns. It finds that, indeed, Ontario broadly fails to meet international best practices for online voting. Our results find the province is broadly *non-compliant* with these best practices, with only 14% of the Council of Europe's 49 standards and 93 implementation guidelines categorized as fully met.

Despite many cybersecurity incidents in Ontario municipalities and worrying findings from

security researchers, the adoption of e-voting in Ontario continues at a breakneck pace. Many municipalities in Ontario have now eliminated the paper ballot altogether. In light of this, this work underscores the urgent need for binding, domestic e-voting standards in Ontario. Without these standards (and compliance with them) it is clear that security risks to Ontario's online elections remain severe and chiefly unmitigated.

Bibliography

- [1] Municipal elections act, 1996. Most recently amended in 2021.
- [2] *Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11*. Committee of Ministers of the Council of Europe, 2004.
- [3] *Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*. Council of Europe Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting, 2017.
- [4] *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. Council of Europe Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting, 2017.
- [5] *Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting*. Council of Europe Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting, 2017.
- [6] Simply voting security information package. <https://www.pertheast.ca/en/about-our-community/resources/2018-Election-Simply-Voting-Security-Information.pdf>, 2018. Provided to the Municipality of Perth East, Ontario.
- [7] *Voluntary Voting System Guidelines VVSG 2.0*. US Election Assistance Commission, 2021.
- [8] Luis Panizo Alonso, Mila Gasco, David Y Marcos del Blanco, José Á Hermida Alonso, Jordi Barrat, and Héctor Aláiz Moreton. E-voting system evaluation based on the council of europe recommendations: Helios voting. *IEEE Transactions on Emerging Topics in Computing*, 9(1):161–173, 2018.
- [9] Paul Barker. Municipalities’ chance of attack ‘critically high,’ misa delegates told. <https://www.itworldcanada.com/article/municipalities-chance-of-attack-critically-high-misa-delegates-told/513327>, 11 2022. Accessed: 2024-03-22.

- [10] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 544–553, 1994.
- [11] Cory Bilyea. Protect our waterways delegation requests paper ballot dgr referendum. *The Hamilton Spectator*, March 2024. Accessed: 2024-03-17.
- [12] Anthony Cardillo, Nicholas Akinyokun, and Aleksander Essex. Online voting in ontario municipal elections: A conflict of legal principles and technology? In *4th International Joint Conference on Electronic Voting*, volume 11759 of *Lecture Notes in Computer Science*, pages 67–83. Springer, 2019.
- [13] Anthony Cardillo and Aleksander Essex. The Threat of SSL/TLS Stripping to Online Voting. In *3rd International Joint Conference on Electronic Voting*, volume 11143 of *Lecture Notes in Computer Science*, pages 35–50. Springer, 2018.
- [14] City of Markham. How to vote online in the 2022 municipal election. YouTube video, <https://www.youtube.com/watch?v=zXUgEfs5gEQ>, October 2022.
- [15] City of Markham, Ontario. Bylaw 2017-20, 2017.
- [16] Jeremy Clark. *Democracy Enhancing Technologies: Toward Deployable and Incoercible E2E Elections*. PhD thesis, University of Waterloo, Waterloo, Ontario, Canada, 2011.
- [17] Jeremy Clark and Aleksander Essex. Internet Voting for Persons with Disabilities - Security Assessment of Vendor Proposals. City of Toronto FOI Request 2014-01543, 2014. Available online: <https://verifiedvoting.org/wp-content/uploads/2020/07/Canada-2014-01543-security-report.pdf>.
- [18] Corporation of the Municipality of South Huron. Schedule a - full agreement simply voting. <https://pub-southhuron.escribemeetings.com/filestream.ashx?DocumentId=633>, 2017.
- [19] Véronique Cortier, Pierrick Gaudry, and Stephane Glondu. *Belenios: a simple private and verifiable electronic voting system*, volume 11565 of *LNCS*, pages 214–238. Springer, 2019.
- [20] Braden L. Crimmins, Marshall Rhea, and J. Alex Halderman. Remotevote and safe vote: Towards usable end-to-end verification for vote-by-mail. In *Financial Cryptography and Data Security. FC 2022 International Workshops*, volume 13412 of *Lecture Notes in Computer Science*, pages 391–406. Springer, 2023.

- [21] Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague. Trust implications of ddos protection in online elections. In *2nd International Joint Conference on Electronic Voting*, volume 10615 of *Lecture Notes in Computer Science*, 2017.
- [22] Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague. Trust implications of DDoS protection in online elections. In *2nd International Joint Conference on Electronic Voting*, volume 10615 of *Lecture Notes in Computer Science*, pages 127–145. Springer, 2017.
- [23] Chris Culnane, Aleksander Essex, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Knights and knaves run elections: Internet voting and undetectable electoral fraud. *IEEE Security & Privacy*, 17(4):62–70, Jul.-Aug. 2019.
- [24] Jean Paul Degabriele. Hiding the Lengths of Encrypted Messages via Gaussian Padding. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1549–1565, 2021.
- [25] David Yeregui Marcos del Blanco and David Duenas-Cid. E-voting system evaluation based on the council of europe recommendations: nvotes. In *5th International Joint Conference on Electronic Voting*, volume 12455 of *Lecture Notes in Computer Science*, pages 147–166. Springer, 2020.
- [26] Elections Canada. The electoral system of canada. <https://www.elections.ca/content.aspx?section=res&dir=ces&document=part2&lang=e>, 2020. Accessed: 2024-04-27.
- [27] Elections Canada Public Enquiries Unit. Election process and secrecy of vote measures. Personal communication, July 2023. Email to James Brunet.
- [28] Jørgen Elklit and Michael Maley. Why ballot secrecy still matters. *Journal of Democracy*, 30(3):61–75, 2019.
- [29] Aleksander Essex. *Cryptographic End-to-End Verifiability for Real-World Elections*. PhD thesis, University of Waterloo, Waterloo, Ontario, Canada, 2012.
- [30] Kai Gellert, Tibor Jager, Lin Lyu, and Tom Neuschulten. On fingerprinting attacks and length-hiding encryption. In *Cryptographers’ Track at the RSA Conference*, pages 345–369. Springer, 2022.
- [31] Micha Germann and Uwe Serdült. Internet voting and turnout: Evidence from Switzerland. *Electoral Studies*, 47:1–12, 2017.

- [32] Nicole Goodman, Iuliia Spycher-Krivososova, Aleksander Essex, and James Brunet. Verifiability experiences in ontario’s 2022 online elections. In *8th International Joint Conference on Electronic Voting*, volume 14230 of *Lecture Notes in Computer Science*, pages 87–106. Springer, 2023.
- [33] Nicole Goodman and Leah C. Stokes. Reducing the cost of voting: An evaluation of internet voting’s effect on turnout. *British Journal of Political Science*, 50(3):1155–1167, 2020.
- [34] J. Alex Halderman. *Practical Attacks on Real-World E-Voting*, chapter 7, pages 143–171. Auerbach Publications, Boca Raton, FL, USA, 2016.
- [35] J Alex Halderman and Vanessa Teague. The New South Wales iVote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity*, pages 35–53. Springer, 2015.
- [36] Helen A Hayes, Nicole Goodman, R Michael McGregor, Zachary Spicer, and Scott Pruyers. The effect of exogenous shocks on the administration of online voting: evidence from ontario, canada. In *7th International Joint Conference on Electronic Voting*, volume 13553 of *Lecture Notes in Computer Science*, pages 70–89. Springer, 2022.
- [37] Hoy J. Cusimano v. toronto (city), 2011 onsc 2527, 2011. Accessed on 2024-03-15.
- [38] Simone Joseph. Advanced voting down in markham, despite added day. https://www.yorkregion.com/news/municipal-elections/advanced-voting-down-in-markham-despite-added-day/article_4a239e02-009c-562b-9913-70e6c4634559.html, October 2014.
- [39] Viktoriia Klymenko. How successfully run your first online election: Interview with ceo of neuvote matthew heuman. <https://news.neuvote.com/how-successfully-run-your-first-online-elections-interview-with-ceo-of-neuvote-matthew-heuman/>, January 20 2023.
- [40] Barbara Latkowski. New dates set for catholic school board trustee election in cambridge. <https://kitchener.citynews.ca/local-news/new-dates-set-for-catholic-school-board-trustee-election-in-cambridge-6055907/>, November 2022.
- [41] Epp Maaten and Thad Hall. *Improving the transparency of remote e-voting: The estonian experience*. Gesellschaft für Informatik e. V., 2008.

- [42] Danielle Manton and Jennifer Shaw. Alternative voting methods update – 2022 municipal & school board election. Technical Report 21-319(CRS), City of Cambridge, 2021.
- [43] Municipality of Central Huron, Ontario. Bylaw 32-2017, 2017.
- [44] Municipality of Central Huron, Ontario. Bylaw 37-2018, 2018.
- [45] F. Pedregosa, G. Varoquaux, A. Gramfort, et al. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.
- [46] Adrià Rodríguez-Pérez. The council of europe’s cm/rec (2017) 5 on e-voting and secret suffrage: time for yet another update? In *7th International Joint Conference on Electronic Voting*, volume 13553 of *Lecture Notes in Computer Science*, pages 90–105. Springer, 2022.
- [47] Timothy Rowlands, Sheruni Ratnabalasuriar, and Kyle Noel. Video gaming, crime, and popular culture. *Oxford Research Encyclopedia of Criminology*, December 2016.
- [48] Royal Canadian Mounted Police. Alberta rcmp concludes investigations. YouTube video, <https://www.youtube.com/watch?v=PZkEeXzaRzU>, March 2024. Quote used is from 21:18.
- [49] Royal Canadian Mounted Police. Alberta rcmp concludes investigations surrounding the 2017 ucp leadership vote. <https://www.rcmp-grc.gc.ca/en/news/2024/alberta-rcmp-concludes-investigations-surrounding-the-2017-ucp-leadership-vote>, March 2024. Accessed: 2024-03-15.
- [50] Canadian Security Intelligence Service. Foreign interference threats to canada’s democratic process. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html>, July 2021. Accessed: 2024-04-20.
- [51] Michael A Specter, James Koppel, and Daniel Weitzner. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US. Federal Elections. In *29th USENIX Security Symposium*, pages 1535–1553, 2020.
- [52] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 703–715. ACM, 2014.

- [53] Swiss Federal Chancellery. Federal chancellery ordinance on electronic voting (oev). <https://www.fedlex.admin.ch/eli/cc/2022/336/en>, 2022. Status as of 1 July 2022.
- [54] Matt Vis. An online ballot error affects 2 ward contests in thunder bay’s municipal election. <https://www.cbc.ca/news/canada/thunder-bay/online-ballot-error-affects-two-thunder-bay-ward-races-1.6609868>, 2022.
- [55] Melanie Volkamer and Robert Krimmer. Requirements and Evaluation Techniques for Online-Voting. In *6th International EGOV Conference*, pages 37–46, 2007.
- [56] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. *Financial Cryptography*, chapter Attacking the Washington, D.C. Internet Voting System, pages 114–128. 2012.

Appendix A

Council of Europe Standards and Implementation Guidelines for E-Voting

This appendix lists the Council of Europe's standards and implementation guidelines for online voting [4, 5], which do not exist in a single document together. These two separate documents are relevant to the thesis and have been combined for ease of reference.

1. The voter interface of an e-voting system shall be easy to understand and use by all voters.
 - (a) The presentation of the voting options on the device used by the voter should be optimised for the average voter who does not have specialised computer knowledge.
 - (b) Voters should be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.
 - (c) Consideration should be given, when developing new IT-products, to their compatibility with existing ones.
2. The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.
 - (a) Voters should be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance.
 - (b) Internet voting interfaces should comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).
3. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

4. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.
5. All official voting information shall be presented in an equal way, within and across voting channels.
 - (a) The electronic ballot used for e-voting should be free from any information about voting options, other than that required by law.
 - (b) If information about voting options is accessible from the e-voting site, it shall be presented in an equitable manner.
6. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.
7. Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.
8. The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.
9. The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.
 - (a) If a voter is allowed to cast an electronic vote multiple times, appropriate measures should be taken to ensure that only one vote is counted.
 - (b) If a voter is allowed to cast a vote by more than one voting channel, appropriate measures should be taken to ensure that only one vote is counted.
 - (c) In all other cases appropriate measures should be taken to prevent a voter from casting more than one vote.
10. The voter's intention shall not be affected by the voting system, or by any undue influence.
 - (a) In the case of remote e-voting, the voter should be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.
 - (b) The e-voting system should not permit any manipulative influence to be exercised over the voter during the voting. In particular, the electronic ballot by which an electronic vote is cast should be free from any unofficial information.

- (c) The e-voting system should introduce all possible measures to avoid any manipulative influence to be exercised over the vote once it has been cast, and it will include measures to allow verification that no such influence was exercised.
 - (d) Where considered necessary, the e-voting system should offer mechanisms (for example, multiple voting) to protect voters from coercion to cast a vote in a specific way.
11. It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.
 12. The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.
 - (a) Voters should be able to alter their choice at any point in the remote e-voting process before casting their vote, or to break off the procedure.
 13. 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.
 14. The e-voting system shall advise the voter if he or she casts an invalid e-vote.
 15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.
 - (a) When using e-voting machines in polling stations, member States should consider the use of paper ballots as a second medium to store the vote for verification purposes.
 - (b) A mandatory count of votes in the second medium in a statistically meaningful number of randomly selected polling stations should be carried out in particular for e-voting machines and optical scanners.
 16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.
 17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.
19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.
 - (a) Voter register data should be clearly separated from voting components.
20. The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.
21. The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify or otherwise gain knowledge of this data.
 - (a) Authentication should use cryptographic mechanisms.
22. Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.
23. An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.
 - (a) Where paper proof of the electronic vote is provided to the voter in a controlled environment, the voter should not be allowed to show it to any other person, or take this proof outside of the polling station.
 - (b) No residual information related to the voter's decision should be displayed after the vote has been cast.
 - (c) In the case of remote e-voting, the voter should be informed of possible risks to voting secrecy and recommended means to reduce them ahead of voting.
 - (d) In the case of remote e-voting, the voter should be informed on how to delete, where it is possible, traces of the vote from the device used to cast the vote.
24. The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.
25. E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.
 - (a) Voter information should be separated from the voter's decision at a pre-defined stage of the counting process.
 - (b) Any decoding required for the counting of the votes should be carried out as soon as practicable after the closure of the voting period.
 - (c) Member States should take the necessary steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

27. Member States that introduce e-voting shall do so in a gradual and progressive manner.
 - (a) A formal feasibility study should be undertaken and published before the selection and implementation of any e-voting technology.
 - (b) Any implementation of e-voting pilots should start well ahead of elections and include essential preparations such as the adoption of detailed regulations, if necessary, for the pilots and system testing.
 - (c) The final version of the e-voting system should be tested before it is used in regular, binding elections.
 - (d) Pilots should be conducted on the basis of clear and comprehensive criteria to evaluate the effectiveness and integrity of the e-voting system, including the transmission of results.

28. Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.
 - (a) The legal framework should include procedures for the implementation of e-voting from set-up and operation to counting.
 - (b) The legal framework should include rules for determination of the validity of an electronic vote.
 - (c) The legal framework should include rules dealing with problems, failures and discrepancies resulting from the use of verification tools.
 - (d) The legal framework should include procedures for the process of data destruction, in particular to align processing, storing and destruction of the data (and equipment) of voting technology with the personal data protection legislation.

- (e) The legal framework should include provisions for domestic and international observers.
 - (f) Legislation should provide for clear timetables concerning all stages of the e-election.
 - (g) The period in which an electronic vote can be cast should not begin before the notification of an election or a referendum.
 - (h) Remote e-voting may start and/or end at an earlier time than the opening of any polling station.
 - (i) The period in which an electronic vote can be cast should not continue after the end of the voting period.
 - (j) The depositing of electronic votes into the electronic ballot box should be allowed for a sufficient period of time after the end of the e-voting period to allow for any delays in the passing of messages over the remote e-voting channel.
 - (k) After the end of the e-voting period, no voter should be allowed to gain access to the e-voting system.
29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.
- (a) Procurement processes for e-voting should be carried out in a transparent manner.
 - (b) Provisions should be made to ensure against possible conflicts of interest of private stakeholders involved in the process.
 - (c) A strict separation of duties shall be maintained and documented.
 - (d) Member States should take appropriate measures to avoid circumstances where the election is unduly dependent on vendor
30. Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.
- (a) A record of the counting process of the electronic votes should be kept, including information about the start and end of, and the persons involved in, the count.
 - (b) The counting of votes should be reproducible. There should be a possibility to obtain sound evidence that the counting procedure has been performed satisfactorily including through an independent recount.
 - (c) Other features that may influence the accuracy of the results of the e-voting system should be verifiable.

- (d) The e-voting system should maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as is required.

31. Member States shall be transparent in all aspects of e-voting.

- (a) The competent electoral authorities should publish an official list of the software used in an e-election.
- (b) Public access to the components of the e-voting system and information thereon, in particular documentation, source code and non-disclosure agreements, should be disclosed to the stakeholders and the public at large, well in advance of the election period.

32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: (a) any steps a voter may have to take in order to participate and vote; (b) the correct use and functioning of an e-voting system; and, (c) the e-voting timetable, including all stages.

- (a) Support and guidance material on voting procedures should be made available to voters.
- (b) In the case of remote e-voting, voter information material should also be available through a different, widely available communication channel.
- (c) Voters should be provided with an opportunity to practise before, and separately from, the moment of casting an electronic vot
- (d)

33. The components of the e-voting system shall be disclosed for verification and certification purposes.

- (a) E-voting systems should generate reliable and sufficiently detailed observation data so that election observation can be carried out.
- (b) Domestic and international observers should have access to all relevant documentation on e-voting processes.
- (c) Member States should make the relevant documentation available to observers, as far as practicable, in a language commonly used in international relations.
- (d) Member States should provide training programmes for domestic and international observer groups.

- (e) Domestic and international observers and the media should be able to observe the testing of the software and hardware.
 - (f) Election observers should have access to all steps of the evaluation and certification process.
34. Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.
35. Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate.
36. Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.
- (a) Member States should establish the aims of certification and the certification methods.
37. Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.
- (a) Member States should determine the apportioning of costs entailed in the certification process. They should define the responsibility, including financial, of the certification body for the quality of their work.
 - (b) Evaluation and certification bodies should have full access to all relevant information and should be allotted sufficient time to carry out the certification process ahead of the election.
 - (c) The mandate of the evaluation and certification bodies should be reconfirmed regularly at prescribed intervals.
 - (d) The conclusions reached in a certification report should be self-explanatory with the information contained in that report.
 - (e) Member States should set and publish clear rules with regard to the disclosure of the final certification report and of all relevant documents, bearing in mind the importance of transparency.

38. The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.
39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.
- (a) The audit system should record times, events and actions, including:
- all voting-related information, including the number of eligible voters, the number of votes cast, the number of valid and invalid votes, the counts and recounts, etc.;
 - any attacks on the operation of the e-voting system and its communications infrastructure;
 - system failures, malfunctions and other threats to the system.
- (b) The e-voting system should maintain reliable synchronised time sources.
- (c) The conclusions drawn from the audit process should be taken into consideration in future e-elections.
40. The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.
- (a) The availability of e-voting services to all voters during the entire e-voting process must be maintained.
- (b) Voters should be promptly informed through appropriate means in case of interruption, suspension or restart of the electronic voting system.
- (c) The voting system does not exclude eligible voters from casting their vote.
- (d) The e-voting system should maintain the availability and integrity of the votes.
- (e) Technical and organisational measures should be taken to ensure that no data is permanently lost in the event of a breakdown or a fault affecting the e-voting system.
- (f) Member States should consider usability throughout the development of security mechanisms.
- (g) Regular checks should be performed to ensure that e-voting system components operate in accordance with the system's technical specifications and that its services are available.

- (h) Key e-voting equipment should be located in a secure area and that area shall, throughout the election or referendum period, be guarded against any unauthorised interference or access.
 - (i) During the election or referendum period, a disaster recovery plan should be in place.
 - (j) It should be possible to check the state of protection of the voting equipment at any time.
 - (k) Sufficient backup arrangements should be in place and be permanently available to ensure that voting proceeds smoothly.
 - (l) The staff concerned should be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.
 - (m) Any data retained after the election or referendum period should be stored securely.
41. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.
- (a) Appointed persons shall have restricted access to e-voting services, depending on their user identity or their user role.
 - (b) While an electronic ballot box is open, any authorised intervention affecting the system should be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the electoral management body and any election observers.
 - (c) Any other critical technical activity should be carried out by teams of at least two people.
42. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.
- (a) Before each election, the equipment should be checked and approved in accordance with a protocol drawn up by the competent electoral authorities.
43. A procedure shall be established for regularly installing updated versions and corrections of all relevant software.
- (a) Formal procedures should be developed for the deployment of software and voting technology configurations.

44. If stored or communicated outside controlled environments, the votes shall be encrypted.

45. Votes and voter information shall be kept sealed until the counting process commences

46. The electoral management body shall handle all cryptographic material securely.

- (a) The private cryptographic keys be should be generated at a public meeting and should be divided in separate parts and shared by at least two people who are unlikely to collude.

47. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.

- (a) The types of incidents are specified in advance by the electoral authorities.
- (b) In case of an incident, competent electoral authorities should take the necessary steps to mitigate the effects of the incident.

48. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

- (a) Printing of voter identification data such as polling cards should be reviewed to ensure security of sensitive data.

49. The e-voting system shall identify votes that are affected by an irregularity.

- (a) The fact that a vote has been cast within the prescribed time limits should be ascertainable.

Curriculum Vitae

Name: James Brunet

**Post-Secondary
Education and
Degrees:** Carleton University
Ottawa, ON
2014-2020 B.C.S.

**Related Work
Experience:** Instructor I
Carleton University, School of Information Technology
2023-2024

Chang School Contract Lecturer
Toronto Metropolitan University
2023

Software Developer
Rewind
2021

Various Technical Roles
New Democratic Party of Canada, Ontario, and Saskatchewan
2019-2021

Campaign Manager and Database Administrator
Clive Doucet for Mayor of Ottawa
2018

Computer Science and Mathematics Teaching Assistant
Carleton University
2015-2018

Publications:

1. Brunet, James, Pananos, Athanasios Demetri, Essex, Aleksander. “Review Your Choices: When Confirmation Pages Break Ballot Secrecy in Online Elections,” *Electronic Voting*, Springer Nature Switzerland, Cham, 2022, pp. 36–52. ISBN 978-3-031-15911-4
2. Goodman, Nicole, Spycher-Krivososova, Iuliia, Essex, Aleksander, Brunet, James. “Verifiability Experiences in Ontario’s 2022 Online Elections,” *Electronic Voting*, Springer Nature Switzerland, Cham, 2023, pp. 87–105. ISBN 978-3-031-43756-4
3. Brunet, James, Essex, Aleksander. “Online Voting in Ontario Municipalities: A Standards-Based Review,” *Electronic Voting*, Springer Nature Switzerland, Cham, 2023, pp. 52–68. ISBN 978-3-031-43756-4