Online Voting in Ontario Municipalities: A Standards-based Review

James Brunet[0000−0001−9018−5106] and Aleksander Essex[0000−0002−0228−0371]

Western University, Canada
{jbrunet8,aessex}@uwo.ca

Abstract. Over two hundred municipalities now offer online voting in Ontario, Canada, representing one of the largest deployments of digital elections worldwide. Many have eliminated the paper ballot altogether. Despite this, no provincial or federal-level standards exist. This gap leaves local election officials to create and apply their own cybersecurity requirements with varying degrees of success.

Until a standard can be developed and adopted, we turn to perhaps the most natural and immediate stand-in: The Council of Europe's (CoE) standards for e-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.

Keywords: Online voting · Standards · Cybersecurity

1 Introduction

Ontario's municipal elections represent some of the highest concentrations of online voting globally. Although turnout by voting-method is not published, a recent study estimated as many as one million voters cast a ballot online in the 2018 Ontario Municipal election [10]. Online voting adoption has grown steadily across the province since 2003. In 2022, the province reached a critical milestone: More than half of Ontario's cities now offer online voting, and many have moved to eliminate the paper ballot altogether.

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?

The answer in Ontario is short but not nearly so sweet: There is no accepted benchmark. 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.

Therefore, the impetus of this work is to provide *some* objective measure for the province to identify critical areas of cyber and democratic risk toward prioritizing areas for improvement. In the absence of a domestic standard, we turn to perhaps the most natural and immediate alternatives: The Council of Europe's Standards for E-Voting (SeV). The SeV offers a set of broad-ranging and well-suited requirements and guidelines for online voting.

In this paper, we conduct a review of online voting in Ontario and analyze compliance against each of the 141 requirements and guidelines of the CoE's SeV. We summarize divergences and identify areas for improvement in hopes of underscoring the urgent need for *domestic* e-voting standards and oversight.

2 Background and Preliminaries

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]

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.[2] 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" [1].

2.1 Terminology

The Council of Europe's Standards of E-Voting (SeV) fall across three main documents [2, 3, 4]. Although distinct from the CoE SeV, the US Voluntary Voting System Guidelines (VVSG) [6] 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:

[1] 2022 Municipal Election - Context. Association of Municipalities of Ontario. Available: https://www.amo.on.ca/municipal-election-statistics

[2] https://www.coe.int/en/web/portal/european-union

Principles. Principles articulate the highest-level priorities. The CoE articulates principles in Section 14 of the explanatory memorandum [2]. 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 [4]. 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 [3]. 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."

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.

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 [15]).

2.3 Related Work

Del Blanco et al. [8] and Luis Panizo et al. [7] performed a cryptographic analysis of the *n*votes and Helios Voting e-voting systems, respectively, on the CoE's requirements for e-voting. This research identified technical limitations with respect to 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.

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.

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 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.

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 1: Summary of compliance

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 Appendix A, but a detailed analysis of each directive is not possible due to space constraints. In this section, we provide a selection of our more interesting findings, with the titles of directives paraphrased and shortened.

4.1 Directive broadly met

`4. Election must be obviously real.` Voters receive official notification by mail of an election, indicating that the election is real. Demonstration/test systems are generally unavailable [9], so voters are unlikely to be confused.

`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" [21]. Specifically, Section 41(2) of the Municipal Elections Act (MEA) specifically outlines how candidates appear on the ballot [15]. 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).

`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. A recent study tested the confirmation pages of Scytl, Simply Voting and Neuvote [9] and found the confirmation pages allow voters to alter their choice, which satisfies implementation guideline 12(a).

`22. Voter list should only be accessible to authorised parties.` We interpret this to mean voter lists. Unlike American states like Ohio,[3] voter lists are not made publicly available and are only accessible to authorized parties (candidates, municipalities, and other election-related authorities).

`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)).

`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 [16].

4.2 Directive Fully Met by Some Cities

`9. Count one vote per voter.` There were several examples of voters receiving multiple voting credentials,[4] 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.

`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) [11]. 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.

`15. Individual verifiability.` Individual verifiability exists for some cities using Scytl or Neuvote, including Markham [13] and Ignace [17], respectively.

[3] https://www6.ohiosos.gov/ords/f?p=VOTERFTP:STWD:::#stwdVtrFiles

[4] https://www.thorold.ca/en/news/thorold-residents-encouraged-to-hold-on-to-all-voter-letters-they-receive.aspx

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 [13]. However, most cities in Ontario use unverifiable voting systems offered by Dominion, Simply Voting, and Intelivote.

`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 [13].

`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. However, 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 [9]. This practice could jeopardize the secrecy of both a voter's unconfirmed choices and their final vote.

`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.[5] In 2018, they entered a contract with Simply Voting at the cost of $1.30 per elector [22], which is well below their threshold of $25,000 for a competitive public procurement process [12].

`32(c). Public demo of e-voting system.` Most vendors do not offer public demos of their e-voting systems [9].

`40(a). No downtime.` Municipalities using Dominion as a vendor experienced service disruptions in 2018 [10] and in 2022.[6][7][8]

`40(i). Disaster recovery plans should exist.` Before 2018, cities generally did not have disaster recovery plans [10] 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.

[5] https://www.centralhuron.ca/en/your-municipal-government/2022-official-municipal-school-board-election-results.aspx
[6] https://twitter.com/NewTecumseth/status/1584694858471690240
[7] https://twitter.com/TwpofScugog/status/1584689666259030016
[8] https://www.thecounty.ca/county_news_notices/online-voting-extended-until-830-pm-on-october-24/

4.3 Directive Partially Met by Most or All Cities

`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.

`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 [2]. 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 Directive Unmet: Meaningful Attempts From Some Cities

`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.

`24. Disclosure of premature results should be prevented by system.` 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) [9, 14], 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.

`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.

4.5 Directive Unmet by Almost All Cities

`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".[9] 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.

`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.

`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..." [19]. Two cities had serious errors which could have been prevented by sufficient procedural steps. Thunder Bay had some voters receive the wrong ballot [23], while Cambridge presented an e-ballot to voters that was missing candidates [18].

`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 [10].

`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.[10][11]

[9] https://votes.clarington.net/en/voters/voter-faqs/
[10] Vote methods in 2018: https://whisperlab.org/ontario-online.csv
[11] Vote methods in 2022: https://elections2022.amo.on.ca/web/en/home

4.6 Directive Unmet by All Cities

`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.

`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 [10].

`23. Proofs of who a voter voted for can't be used by third parties.` The verification method employed by Scytl shows the voter which choice they selected [13]. Any third party, given a QR code and a voter's credentials, could verify this proof themself. Most other vendors offer no proof.

`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.[12][13] 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 [5].

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 [10].

`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)).

`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)).

`31, 31(a-b), 33, 33(a-f), 34. Transparency, disclosure, and observation` Private vendors are not subject to access-to-information law, have

[12] https://twitter.com/ClaringtonON/status/1555184785089347596

[13] https://www.baytoday.ca/2022-municipal-election-news/election-officials-easing-concerns-about-online-voting-system-5944887

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.

`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.

`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.

4.7 Directive Unmet Due to Failure Within Provincial Jurisdiction

`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 [20].

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 [15]. 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.

4.8 N/A—Outside of Expertise

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.

4.9 N/A—Not Applicable to Ontario

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.

4.10 N/A—Not Applicable to E-voting

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.

4.11 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 reports). 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.

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 their own 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 [1]. 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" [1]. Independent verification such as cryptographic end-to-end verification (E2E-V) would address many unmet directives.

References

[1] Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11. Committee of Ministers of the Council of Europe (2004)
[2] 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), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84
[3] 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), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b
[4] 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), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f
[5] Simply voting security information package (2018), https://www.pertheast.ca/en/about-our-community/resources/2018-Election-Simply-Voting-Security-Information.pdf

[6] Voluntary Voting System Guidelines VVSG 2.0. US Election Assistance Commission (2021)
[7] Alonso, L.P., Gasco, M., del Blanco, D.Y.M., Alonso, J.Á.H., Barrat, J., Moreton, H.A.: 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)
[8] del Blanco, D.Y.M., Duenas-Cid, D.: E-voting system evaluation based on the council of europe recommendations: nvotes. In: E-VOTE-ID. pp. 147–166 (2020)
[9] Brunet, J., Pananos, A.D., Essex, A.: Review your choices: When confirmation pages break ballot secrecy in online elections. In: Electronic Voting: 7th International Joint Conference, E-Vote-ID 2022, Bregenz, Austria, October 4–7, 2022, Proceedings. pp. 36–52. Springer (2022)
[10] Cardillo, A., Akinyokun, N., Essex, A.: Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In: International Joint Conference on Electronic Voting (E-Vote-ID). vol. 11759, pp. 67–82 (2019)
[11] Cardillo, A., Essex, A.: The Threat of SSL/TLS Stripping to Online Voting. In: International Joint Conference on Electronic Voting. pp. 35–50. Springer (2018)
[12] Central Huron: Bylaw 37-2018 (2018), https://centralhuron.civicweb.net/document/50603/
[13] City of Markham: How to vote online in the 2022 municipal election. YouTube video (October 2022), https://www.youtube.com/watch?v=zXUgEfs5gEQ
[14] Clark, J., Essex, A.: 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
[15] Government of Ontario: Municipal elections act, 1996, s.o. 1996, c. 32, sched. (1996), https://www.ontario.ca/laws/statute/96m32
[16] Joseph, S.: Advanced voting down in markham, despite added day. Webpage (October 2014), https://www.yorkregion.com/news/municipal-elections/advanced-voting-down-in-markham-despite-added-day/article_4a239e02-009c-562b-9913-70e6c4634559.html
[17] Klymenko, V.: How successfully run your first online election: Interview with ceo of neuvote matthew heuman. Webpage (January 20 2023), https://news.neuvote.com/how-successfully-run-your-first-online-elections-interview-with-ceo-of-neuvote-matthew-heuman/
[18] Latkowski, B.: New dates set for catholic school board trustee election in cambridge (November 2022), https://kitchener.citynews.ca/local-news/new-dates-set-for-catholic-school-board-trustee-election-in-cambridge-6055907/
[19] Manton, D., Shaw, J.: Alternative voting methods update – 2022 municipal & school board election. Tech. Rep. 21-319(CRS), City of Cambridge (2021), https://www.cambridge.ca/en/elections/resources/Alternative-Voting-Methods-Update.pdf
[20] Markham: Bylaw 2017-20 (2017), https://pub-markham.escribemeetings.com/filestream.ashx?documentid=9670
[21] Ontario Superior Court of Justice: Cusimano v. toronto (city), 2011 onsc 2527 (canlii) (2011), http://canlii.ca/t/fl5pg
[22] The Corporation of the Municipality of Central Huron: Bylaw 32-2017 (2017), https://centralhuron.civicweb.net/document/45563/

[23] Vis, M.: An online ballot error affects 2 ward contests in thunder bay's municipal election. CBC News (2022), https://www.cbc.ca/news/canada/thunder-bay/online-ballot-error-affects-two-thunder-bay-ward-races-1.6609868

A Summary of Analysis

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

Continued on next page...

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

●: 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