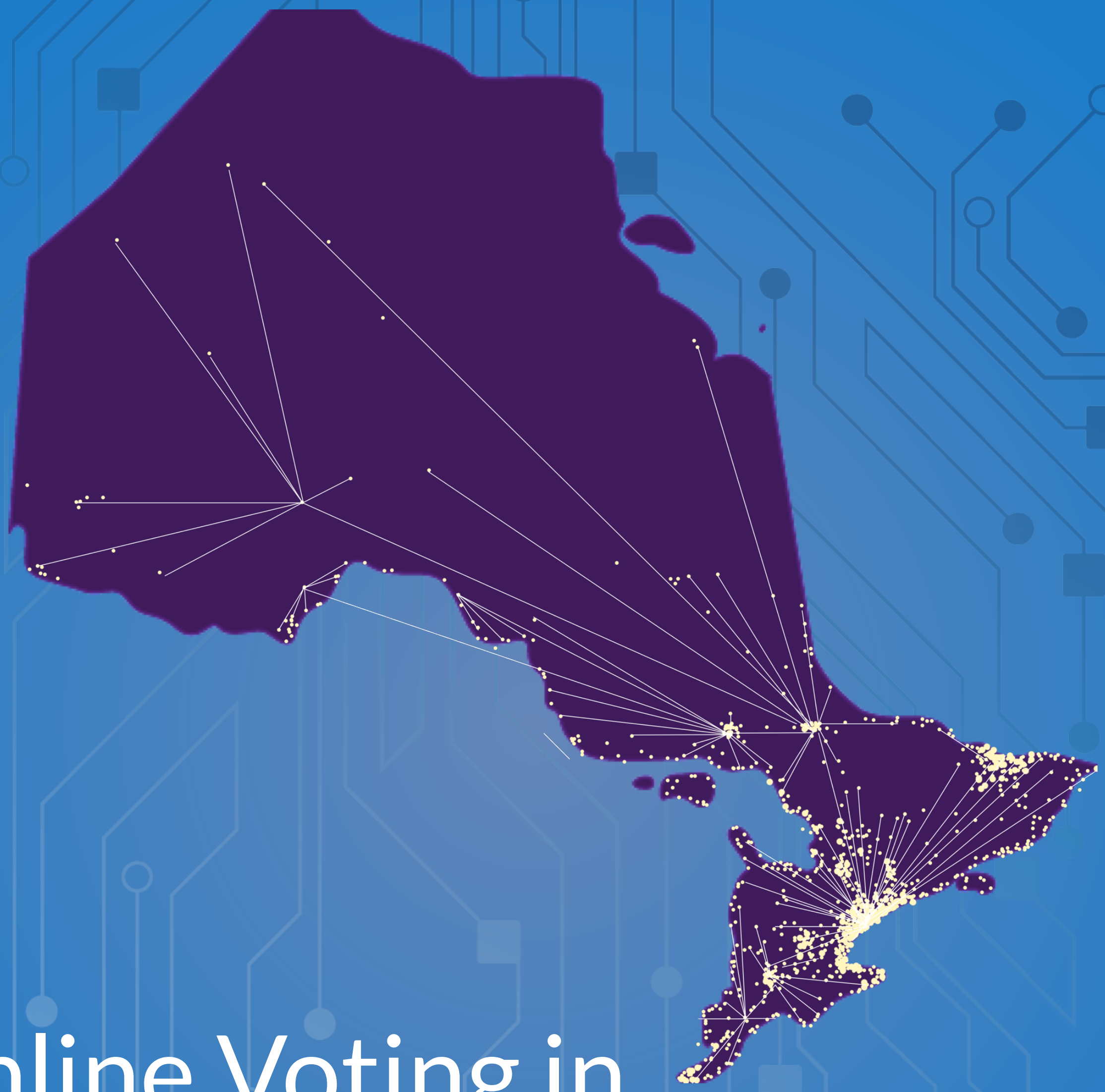


Online Voting in Ontario's Municipal Elections

A Conflict of Legal Principles and Technology?

Authored by

Aleksander Essex, PhD., P.Eng.
Associate Professor
Department of Electrical and Computer Engineering
Western University, Canada

Anthony Cardillo
Department of Electrical and Computer Engineering
Western University, Canada

Nicholas Akinyokun
School of Computing and Information Systems
The University of Melbourne, Australia

WHISPER LAB.org

Western Engineering

PUBLICATION NOTE

An extended abstract of this report was presented at the Fourth International Joint Conference on Electronic Voting (E-Vote-ID) in Bregenz, Austria, October, 2019. It won the Best Paper Award in the Track on Security, Usability and Technical Issues.

Cite the extended abstract as:
Anthony Cardillo, Nicholas Akinyokun, and Aleksander Essex. Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?. In: Krimmer R. et al. (eds) Electronic Voting. E-Vote-ID 2019. Lecture Notes in Computer Science, vol. 11759, pp. 67-82, 2019.

Cite this full report as:
Anthony Cardillo, Nicholas Akinyokun, and Aleksander Essex. Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? Whisper Lab Research Report, Western University, 2020. Available online: `https://whisperlab.org/ontario-online.pdf`

Acknowledgments

We are grateful to a many individuals in Ontario and beyond for helpful conversations and important insights. Special thanks to Jane Buchanan for her tireless effort searching municipal documents.

Thanks to Joe Abley, Richard Ackerman, Tony Adams, Matt Bernhard, Kevin Creechan, Faye and Ron Ego, Josh Franklin, Nicole Goodman, Jared Marcotte, Beata Martin-Rozumiłowicz, John Meraglia, Scott Richie, Matt Saunders, Cameron Shelley, Ken Strauss, Dave Suffling, Vanessa Teague, Anne Walkinshaw, Susan Watson, Uli Watkiss.

Thanks to the Association of Municipal Managers, Clerks and Treasurers of Ontario (AMCTO) for giving us several opportunities to share the results of this study with their membership. Finally, we wish to thank the numerous voters and candidates of the 2018 Ontario municipal election who contacted us to share their concerns.

This work is dedicated to the voters and candidates of future Ontario municipal elections.

ABOUT THE AUTHORS

Aleksander Essex

Aleksander Essex is an associate professor of software engineering at Western University, and head of the Western Information Security and Privacy Research Lab. His research specialization is cybersecurity and applied cryptography, and he is an internationally recognized expert on the cybersecurity of electronic and online voting.

Since 2007, his research has focused on developing and deploying advanced technological methods for evidence-based elections, as well as identifying, reporting, and fixing vulnerabilities in existing election systems. In Canada, he has worked with federal, provincial, territorial and municipal governments to promote the development of secure election technology, standards, and practices. He is a member of the Election Verification Network, an international professional society of election technology experts.

Anthony Cardillo

Anthony Cardillo is a masters candidate in the Department of Electrical and Computer Engineering at Western University. His research focuses on computation on encrypted data using homomorphic encryption in the health data privacy setting. He is supervised by Prof. Essex.

Nicholas Akinyokun

Nicholas Akinyokun is a Ph.D. candidate in the School of Computing and Information Systems at The University of Melbourne, Australia. His research focuses on secure multi-party computation for evidence-based elections. He his supervised by Prof. Vanessa Teague.

CONTACT INFORMATION

For questions, corrections or more information about this report, please contact:

Aleksander Essex
Department of Electrical and Computer Engineering
Western University
London, ON, Canada, N6A 5B9

☎ (519) 661-2111 ext. 87290
✉ aessex@uwo.ca
🌐 `https://essex.cc`
🐦 @aleksessex

EXECUTIVE SUMMARY

Despite Ontario having one of the largest concentrations of online voters globally, its use is not governed by any federal or provincial cybersecurity standard. This has left many municipalities to make decisions largely in isolation, relying on private for-profit vendors to set their own bar for cybersecurity and public accountability.

This report presents the first comprehensive study of the cybersecurity of online voting in the context of Ontario's 2018 municipal election. Our key findings include:

- The only comprehensive accounting of online voting adoption, vendor partnerships, and the extent of municipalities affected by emergency extensions to the voting period on election night,
- Identification and discussion of cybersecurity incidents and non-best practices observed in the election, including weak voter authentication, poor transparency and accountability of election results, and a general lack of disaster-preparedness, which resulted in nearly one million voters receiving an emergency extension to the voting period due to a misconfiguration in the online infrastructure on election night,
- A study of ballot secrecy demonstrating that up to 50% of the online voters in the 2018 election were uniquely re-identifiable by their login credentials,

From these observations, we question whether the democratic and legal principles of the *Municipal Elections Act* are being adequately protected by the technology deployed in practice and provide a series of concrete recommendations for municipalities and the province, including the development of mandatory minimum cybersecurity standards of online voting.

CONTENTS

1 Introduction 7

2 Background 7

2.1 Online Voting in Ontario Municipalities 7

2.2 Legal Context 8

3 Election Statistics 9

3.1 Initial Survey of Available Data 9

3.2 Data Collection Methodology 10

3.3 Results: Who Used Online Voting? 11

4 Key Observations and Findings 13

4.1 Disaster Preparedness 13

4.2 Voter Authentication 15

4.3 Transparency and Accountability 16

5 Other Observations and Findings 18

5.1 Cybersecurity claims 18

5.2 Voter Assistance in an Unsupervised Setting 23

5.3 Limitation of Liability 23

5.4 Security of Voter Computers 23

5.5 Scrutineering in an Online Setting 25

5.6 Data Ownership 25

6 Analysis of Voter Confidentiality and Ballot Secrecy 26

6.1 Re-identifying Voters with City and Date of Birth 26

7 Recommendations 28

8 Conclusion 31

A 2018 Online Voting Use By Municipality 34

B Municipalities Declaring Emergency Voting Extensions 45

C Dominion's Election Night Statement 46

1 INTRODUCTION

In an era characterized by foreign interference in national elections, it can be easy to lose sight of the cybersecurity of elections held at the municipal level. With much of our attention squarely focused on state-level threat actors, we must occasionally remind ourselves of a more fundamental threat to our democracies: loss of confidence in the process itself. This idea is summarized expertly by the Supreme Court of Canada:

> Maintaining confidence in the electoral process is essential to preserve the integrity of the electoral system, which is the cornerstone of (our) democracy. ... if (electors) lack confidence in the electoral system, they will be discouraged from participating in a meaningful way in the electoral process. More importantly, they will lack faith in their elected representatives. Confidence in the electoral process is, therefore, a pressing and substantial objective.[1]

In this report, we study online voting in the context of Ontario's 2018 municipal elections in which as many as one million voters cast a ballot online. In the absence of almost any federal or provincial government standards or oversight, municipalities and their private for-profit vendors are primarily left to set their own bar for cybersecurity and public accountability in their elections.

We present several observations about the election and question whether the associated practices align with the legal principles established in case law. We believe these observations will prove significant to municipalities, since, as the Chief Electoral Officer of Ontario recently pointed out:

> As the public becomes more informed about software, malware, and manipulation of technology data systems, they are increasingly interested in knowing exactly how election technology preserves the integrity of our electoral process and the confidentiality of their personal information [6].

This leads to the central thesis of this work: purposeful, malicious interference, or fraud is not necessary to undermine an election. Nor is the honest discharge of an election sufficient to prevent it. Given enough time, a seed of doubt in an otherwise faithfully executed election may eventually grow to accomplish what even the best threat actor cannot. With the goal of preventing this outcome, we hope this work will serve as an encouragement to Ontario municipalities and others contemplating online voting to develop standards to address these issues.

2 BACKGROUND

Canada does not offer online voting at the federal level, and cybersecurity is a significant factor in that position. The parliamentary Special Commission on Electoral Reform (ERRE) reviewed the possibility of online voting in 2016 and recommended against its introduction on cybersecurity grounds [22, 3, 4].

2.1 Online Voting in Ontario Municipalities

Municipalities in the provinces of Ontario and Nova Scotia have held online elections since 2003 [14]. Since then, adoption in Ontario has followed an exponential trend, nearly doubling with each election cycle. As

[1] Harper v. Canada (Attorney General), [2004] 1 SCR 827, 2004 SCC 33 (CanLII). Available online: http://canlii.ca/t/1h2c9

of the 2018 municipal election, we observed 45% of municipalities (accounting for 29% of the province's 9.4 million voters) offered online voting. Furthermore, 33% of municipalities (accounting for 16% of all voters in Ontario) eliminated paper ballots completely. While hard numbers of turnout by voting method have not been made publicly available, we estimate the number of Ontario voters casting a ballot online between 2-4 times higher than Estonia (see Section 3.3).

Despite concerns about the use of online voting, the Communications Security Establishment (CSE) assesses threats to municipal elections as "very likely to remain at its current low level," [3], which is often cited by municipal councils and clerks favoring the adoption of online voting. While the report considers conventional threat actors (nation-states, hacktivists, cybercriminals, terrorist groups, political actors), it overlooks others, such as election officials, system manufacturers, and system operators (cf. [21]). Nor does it consider the inherent threat to confidence posed by the use of non-transparent election technology.

Furthermore, no technical standards currently exist within Canada for designing, testing, or certifying online voting systems, nor auditing or otherwise independently verifying the result they produce. Nor do the federal or provincial governments provide guidance on the procurement and operation of such systems. As we discuss in Section 3.1, Ontario offers almost no oversight to the degree that they do not even track which municipalities offer online voting.

Prior to this study, the only publicly available figures were self-reported by vendors, which we later determined were overstated in each instance. See Section 3.2 for discussion.

Finally, the population difference between the largest and smallest municipalities in Ontario is *four* orders of magnitude. While some municipalities have the resources to perform security reviews of vendor proposals,[2] others rely almost entirely on their vendors for cyber-expertise.

2.2 Legal Context

A commonly used expression in Ontario municipal politics is that "cities are creatures of the province," which references the fact that the province legislates their existence.[3] Municipalities are categorized by three tiers: single, lower, and upper. Upper-tier municipalities correspond to counties or regional municipalities, which consist of multiple lower-tier municipalities. Municipal councils exist at all three tiers; however, elections are only conducted by single- or lower-tier municipalities. The composition of upper-tier councils is either determined automatically, e.g., as a council of all the mayors of the constituent lower-tiers (as in Bruce County) or by a direct ballot question in the constituent lower tier-elections (as in the election of the Regional Chair of Durham).

Ontario has 444 municipalities: 30 upper-tier, and 414 lower- and single-tier. In the 2018 Ontario Municipal Election held on October 22nd, each single- and lower-tier municipality was responsible for organizing and delivering its own independent election. This means up to 414 municipal councils made up to 414 individual decisions about the use of online voting in their election.

[2] Security Assessment of Vendor Proposals, Toronto, 2014. Available online:https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf

[3] Municipal Act, 2001, S.O. 2001, c. 25. Available online: https://www.ontario.ca/laws/statute/01m25

Municipal Elections Act (MEA).

The main piece of legislation governing municipal elections in Ontario is the Ontario Municipal Elections Act (MEA).[4] Although online voting is not explicitly mentioned in the MEA, it allows a municipal council to pass by-laws authorizing the use of "an alternative voting method, such as voting by mail or by telephone, that does not require electors to attend at a voting place in order to vote," (MEA sec. 42). Additionally, it grants municipal clerks the power to establish procedures for alternative voting methods.

Whereas the MEA provides extensive language surrounding the delivery of paper-ballot elections and other electoral matters such as the use of rank-choice ballots, it provides no guidance regarding how to deliver an online election. The Act does not even contain the words "online," or "internet."

This contrast between specificity for paper-ballot in-person elections on the one hand and ambiguity toward online voting on the other leads to an apparent contradiction in places between the letter of the law, and the technology being used in practice. For example, the Act requires that "no person shall communicate any information obtained at a voting place about how an elector intends to vote or has voted," (MEA, Sec. 49 (2)c). However, the act of casting a ballot in an online voting system communicates—in the literal network communication sense—information to the online system about how an elector has voted.

Legal Principles.

Democratic and legal principles provide an important lens through which to interpret the use of technology in elections (cf. [1]), especially in the absence of technical standards. The principles of the MEA are not included in the MEA itself, but have been inferred from its provisions and set out in case law as follows:[5]

- **Ballot secrecy**. The secrecy and confidentiality of the voting process is paramount,
- **Fairness**. The election shall be fair and non-biased. Voters and candidates shall be treated fairly and consistently,
- **Accessibility**. The election shall be accessible to the voters,
- **Integrity**. The integrity of the voting process shall be maintained throughout the election,
- **Certainty**. There is to be certainty that the results of the election reflect the votes cast,
- **Eligibility**. Valid votes are counted and invalid votes are rejected so far as reasonably possible.

3 ELECTION STATISTICS

3.1 Initial Survey of Available Data

Several months before the election, we set out to obtain a list of which cities were intending to use online voting. We wrote to the Ontario Ministry of Municipal Affairs and Housing (MAH) in March 2018 and were surprised to discover this list did not exist. Although the MEA requires local municipal councils to formally pass a by-law authorizing the use of an alternative voting method in the year prior to the election, we

[4] Municipal Elections Act, 1996, S.O. 1996, c. 32, Sched. Available online: https://www.ontario.ca/laws/statute/96m32

[5] Cusimano v. Toronto (City), 2011 ONSC 2527 (CanLII) at para. 67. Available online: http://canlii.ca/t/fl5pg

were informed in an email response that "municipalities are not required to declare their intentions to the province ... the Ministry does not have a list of municipalities that will be using internet voting in the 2018 municipal election." Several of the vendors had commented publicly on the total number of their municipal clients, but none offered a breakdown. One of our colleagues requested such a breakdown from one of the vendors, but they refused to provide it. It was evident that we would need to collect the data ourselves.

3.2 Data Collection Methodology

Correcting the Municipal List.

Our first step was to obtain a complete list of Ontario's 444 municipalities, their tier-status, and associated URL. We consulted MAH's online list[6] and quickly discovered many URLs were incorrect or outdated. For example, many municipalities had switched from the older `city.on.ca` form to the newer `city.ca` form. Some cities no longer owned the URL listed. For example, the URLs listed for Mattawan and Larder Lake directed to Japanese-language websites. We had to inspect each of the 444 URLs for correctness manually. We wrote to MAH around the time of the election and received an acknowledgment that they would undertake to update their list. Six months later, many of the errors we identified remained uncorrected.

Tracking Down Voting Website URLs.

Our next step was to determine which municipalities were planning to use online voting, which vendor they contracted, and the URL of the voting website. We were concerned that finding the URLs would be challenging, since many municipalities we observed made it a practice never to list it anywhere online, revealing them only in the voter information package mailed to voters before the election. Sample voter information packages found online used a placeholder URL (e.g., `anytown.election.ca`, and candidate social media fairly consistently respected this approach. We believe the practice of concealing URLs was meant as a cybersecurity protection to make the voting site harder to find by non-residents.

We made inquiries with colleagues in the province about the URL of the voting site in their respective cities and observed a trend in which vendors were encoding a municipality's voting website either into sub-domain (e.g., Intelivote used the form `city.evote2018.ca`), or sub-directory (e.g., Dominion used the form `intvoting.com/city`). We then wrote a collection of automated scripts that used the municipal list to search for the existence of voting sites based on the particular URL form a vendor was using. For municipalities encoded into sub-domains, we performed passive DNS lookups. For names encoded as sub-directories, we attempted to fetch the HTTP header from the server and inferred whether the page existed from the response code.

For any municipalities not captured by the bulk search, we conducted a labor-intensive manual web search of online municipal documents, including meeting minutes of councils and voter accessibility documentation. This allowed us to identify municipalities using custom domain names (e.g., `kenoravotes.ca`), and abbreviations (e.g., Elizabethtown-Kitley used `ektwp.evote2018.ca`). The only URL we were not able to find with this approach was Markham's, who were partnered with Scytl, so there was no obvious way to infer the URL from others. Furthermore, staff and candidates made a seemingly flawless effort of not mentioning the URL in online documents, social media, etc. Ultimately, however, we found it

[6] List of Ontario Municipalities. Ontario Ministry of Municipal Affairs and Housing. http://www.mah.gov.on.ca/page1591.aspx

(evote.markham.ca) by searching certificate transparency logs.

Cross-validation and Corrections.

After the election, the Association of Municipalities of Ontario (AMO) published a list of municipalities broken down by election results, number of eligible voters, and voting methods offered.[7] Rather than being made available as a single downloadable data file, the figures were spread across 444 individual web-pages, which we scraped in order to cross-validate against our list.

We found a few mistakes in the AMO list. For example, the municipalities of Belleville, Bracebridge, and Timmins were reported as not using online voting when, in fact, they did. The township of Machin was reported as using online voting when it did not. We shared this information with the AMO. We also discovered three municipalities with active websites on Intelivote's domain for which no election was held as the races were acclaimed. We also initially falsely concluded that Newmarket had contracted Intelivote since there was an active website on the evote2018.ca domain. The Newmarket deputy clerk later confirmed they contracted Scytl instead.

Vendor Figures.

To our knowledge none of the vendors publicly reported which municipalities they contracted with, and at least one vendor explicitly refused to provide that information to a fellow researcher. Three of the four vendors, however, self-reported the number of municipalities whose elections they were running. In each of these cases we observed the vendor reported figures were *higher* than what was observed.

For example, Intelivote Systems stated 194 municipalities would be offering online voting in the 2018 election, which was almost 10% higher than actual number.[8]

Dominion's election night statement (see Appendix C) claimed "51 Ontario municipalities using Dominion's Internet Voting portal experienced slow traffic." Our analysis found that Dominion only had 49 municipal clients (see Appendix B)/ of which only 43 experienced a slowdown.

Finally, Scytl was involved in 100 actual elections, however evidently counted three unexecuted contracts in the figures on its website: "103 municipalities ... leveraged Scytl's online & phone voting technology."[9] They go on to claim "Scytl's online and phone voting solution positions itself as the number one technology used in Ontario elections." While the Scytl/Intelivote partnership accounts for over 50% of the market share by municipality, our analysis shows Dominion leads market share in eligible voters (see Table 2), which is a key determinant in overall dollar cost of a contract.

3.3 Results: Who Used Online Voting?

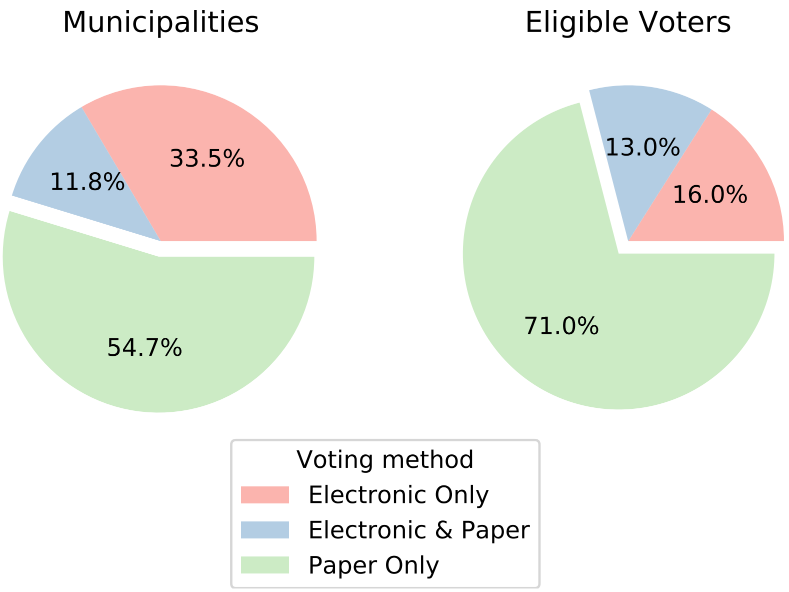
Of the 444 municipalities, 30 upper-tier municipalities do not hold elections, and 23 single-/lower-tier municipal councils were acclaimed and therefore did not run an election. In total there were 391 elections involving 9,444,628 eligible voters. Of those, 177 offered an online voting option, of which 131 were completely paperless. Our full dataset is available for download online.[10]

[7] https://elections.amo.on.ca

[8] The New Frontier of Online Voting. The Agenda with Steve Paikin. TV Ontario. Television broadcast Sept. 19, 2018. Available online: https://www.tvo.org/video/the-new-frontier-of-online-voting

[9] https://www.scytl.com/en/customers/ontario-municipalities/

[10] https://whisperlab.org/ontario-online.csv



Voting method	Municipalities		Eligible Voters	
Electronic ballot only	131	(33.5%)	1,512,076	(16.0%)
Electronic and paper	46	(11.8%)	1,230,019	(13.0%)
Paper ballot only	214	(54.7%)	6,702,533	(71.0%)
Total	391		9,444,628	

Table 1: Voting methods offered in the 2018 Ontario municipal election.

Table 1 shows the number of municipalities and eligible voters by voting method. These consisted of electronic ballot options (online and telephone ballot casting), paper ballot options (incl. optical-scan and postal mail-in), or a combination of options. Combining the AMO's population data with our observations, our results show that online voting was available to approximately 2.74 million voters, or 29% of the voting population. Of these, approximately 1.51 million voters, or 16% of the voting population experienced a completely paperless ballot, cast either online or by telephone.

Most municipalities did not report turnout categorized by voting method. However, if we combine our numbers with the AMO's province-wide turnout rate of 38.2%, we estimate the total number of voters who cast ballots online to be between 0.5–1 million, which is approximately 2–4 times the online ballots cast in the 2019 Estonian parliamentary elections.[11]

We observed 4 vendors active in the 2018 Ontario election: Dominion Voting Systems,[12] Intelivote Systems,[13] Simply Voting,[14] and Scytl.[15] Intelivote and Scytl worked together in partnership, although the extent of their business relationship remains unclear to us. Though ostensibly distinct business entities, we observed both Scytl Canada Inc. and Intelivote Systems Inc. have a registered office at the same mail-

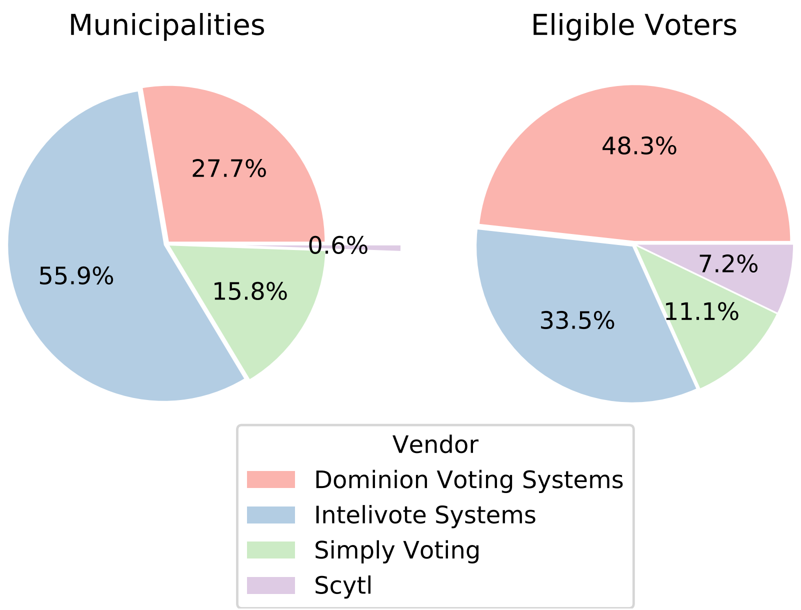
[11] https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

[12] https://www.dominionvoting.com/

[13] http://www.intelivote.com/

[14] http://www.simplyvoting.com/

[15] https://scytl.com/



Vendor	Municipalities		Eligible Voters	
Dominion Voting Systems	49	(27.7%)	1,323,194	(48.3%)
Intelivote Systems	98	(55.4%)	860,985	(31.4%)
Simply Voting	28	(15.8%)	304,479	(11.1%)
Scytl	2	(1.1%)	253,437	(9.2%)
Total	177		2,742,095	

Table 2: Online voting market share in the 2018 Ontario municipal election.

ing address in Dartmouth, NS. Additionally, we observed a considerable portion of Intelivote's web content (Javascript, images) and infrastructure (IPs, domains) appears to have been provided by Scytl. Of the municipalities offering online voting, Table 2 shows the relative market share. A complete list of Ontario municipalities and online voting adoption information is provided in Appendix A.

4 KEY OBSERVATIONS AND FINDINGS

In this section we present three key election findings and discuss their relationship to the MEA principles.

4.1 Disaster Preparedness

One open question was how municipalities were preparing for the possibility of a disaster in the online voting infrastructure (accidental or otherwise), especially in the absence of standards. Our initial examination of municipal documents found no mention of a disaster recovery plan. We raised this issue in the media six months prior to the election [9]. Several clerks were also interviewed but "could not provide a disaster plan to be implemented in case the election is hacked, or irregularities tip the balance in favor of a candidate who should not have been elected." The clerk of Sarnia acknowledged, "I don't have a disaster plan in place right now, I'd have to talk to my vendor about that." The clerk for St. Thomas added, "We're hoping nothing does happen."

Election night emergencies.

As it turned out, something significant did happen. Starting around 6 p.m. on election night, the voting websites of 43 municipalities experienced a dramatic slowdown. Just before 6 p.m., we performed a network capture of the login page for Hanover's voting site, and after 2 minutes the page load timed out. Although the static content appeared to load, the dynamic content loads dragged on, and some eventually timed out.

In the face of an unavailable voting website, and with many affected municipalities without any paper ballot option as a back-up, many clerks made the extraordinary decision to declare emergencies to extend the voting period. In some cases, voting was extended later into the evening by 1-2 hours. The majority of affected municipalities, however, extended voting by a full 24 hours [24, 16].

A statement by Dominion (see Appendix C) on the night of the election attributed the slowdown to their co-location provider (an IT sub-contractor) "placing an unauthorized limit on incoming voting traffic that was roughly 1/10th of the system's designated bandwidth." The statement claimed "approximately 51 municipalities" experienced the slowdown. However, our analysis shows Dominion only ran 49 elections, of which 6 experienced no slowdown on account of having offered online voting during the advance voting period only. Dominion did not disclose the names of the affected cities, so we assembled this list manually by examining multiple news sources and municipal websites.[14] The number of municipalities and affected voters are shown in Table 3. A complete list of municipalities who extended voting periods is provided in Appendix B

Five months after the election we were invited to present preliminary results of this paper to the Association of Municipal Managers, Clerks and Treasurers of Ontario (AMCTO). We spoke to several clerks and a representative from Dominion. None were willing or able to provide any explanation for the events that lead to the co-location provider's bandwidth restriction, nor even the provider's identity.

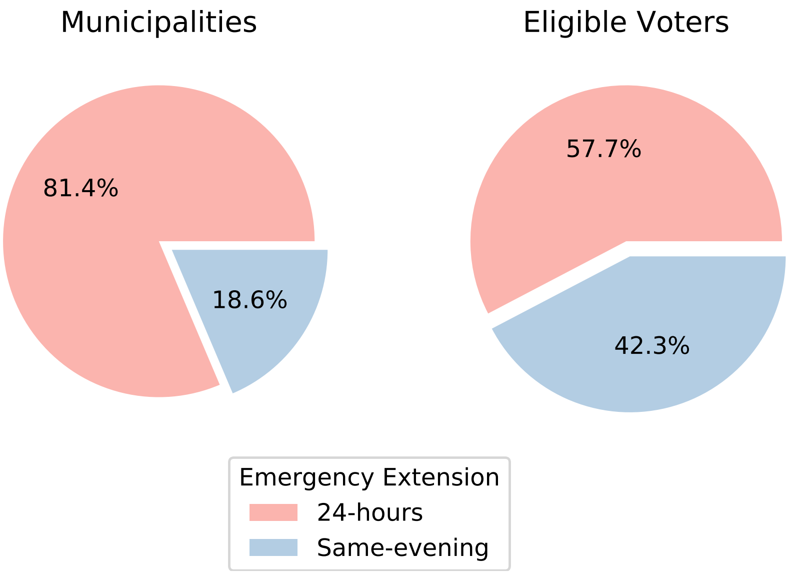
Sudbury's post-election report, released over three months later finally explained the issue:[16]

> [T]he slowdown and timeout issues were caused by a miscommunication between Dominion and the service provider regarding the port bandwidth and the limits placed upon it. The bandwidth requested by Dominion was 1Gbs; however, it was revealed that this was mistakenly taken by the service provider to be the upper potential bandwidth limit not the continuous bandwidth standard. During the slowdown of the system the bandwidth limit was set to only 100 Mbs, which Dominion indicated was approximately only half of the expected peak requirement.

Conflict with principles.

The outage may contradict the accessibility principle on the basis that the voting websites became inaccessible to voters. The unexpected nature of the outage may contradict the fairness principle on the basis that

[16] City of Sudbury. Post Election Report. Jan 21, 2019. Available: https://agendasonline.greatersudbury.ca/index.cfm?pg=feed&action=file&agenda=report&itemid=25&id=1312



Emergency Extension	Municipalities	Eligible Voters
24-hour extension	35	575,022
Same-evening extension	8	422,085
Total	43	997,107

Table 3: Emergency extensions due to Dominion's election night slowdown

the emergency extensions to the voting periods allowed some voters an additional day to form a decision relative to those who had cast their ballots just prior to the slow-down.

4.2 Voter Authentication

Voter lists at the municipal level are largely derived from the Municipal Property Assessment Corporation (MPAC), whose primary business is not voter list management. This mismatch of focus has lead to inaccurate municipal voter lists over the years, and numerous news stories ran prior to the election on the subject. Because the lists are derived from property ownership, we heard anecdotal accounts of rental tenants who did not receive their online voting login credentials, whereas non-resident adult children away in college did. Other accounts described land owners of multiple properties receiving multiple login credentials. One news story reported a deceased dog in the town of Mono received a PIN [8].

Online voting credentials.

The primary credential needed to cast a ballot online consisted of a knowledge factor (a PIN and/or ID) transmitted to the voter in a voter information package via postal mail. To our knowledge, the sole exception was the city of Cambridge, which sent PINs via email. In almost all cases a second knowledge factor (date of birth) was required. See Table 4 for a breakdown of credentials used by the vendor.

The use of single credential for voter authentication is inadvisable since access to the voter information

Vendor	Primary credential (mailed)	Secondary credential
Dominion	13-digit ID & 8-digit PIN	Date of birth
Intelivote	16-digit PIN	Date of birth
Scytl	16-digit PIN	Date of birth
Simply Voting	9-digit PIN	Date of birth

Table 4: Credentials needed to vote online

package is sufficient to cast a ballot on another's behalf. Furthermore, some voters observed that the PINs were legible through the envelope when held up to bright light. See Figure 1. In order to mitigate this risk, most municipalities required a date of birth as a secondary credential. Note that authentication is still considered single-factor (as opposed to multi-factor) authentication since both credentials are knowledge factors.

Dates of birth, however, make a poor login credential for several reasons. Aside from the significant privacy implications (which we discuss in Section 6), they are low entropy, cannot be changed, and typically are not very secret, especially when considering one's co-habitants (i.e., friends and family) are potential threats. Aside from the widespread practice of sharing dates of birth on social media websites, some US states such as Ohio include dates of birth in voter registries which are freely available for download online.

Much of the voting literature on eligibility and authentication focuses on threats like coercion and vote selling. In practice, however, it appears that a far more pervasive version of these threats is also more casual.

Voting on someone else's behalf is an offense under the MEA. Nevertheless, we heard anecdotal accounts from several independent sources of parents who voted on behalf of children living in another city, or people who voted on behalf of their spouse while they were at work. We also heard accounts of individuals gifting their unopened voter information packages to friends and family.

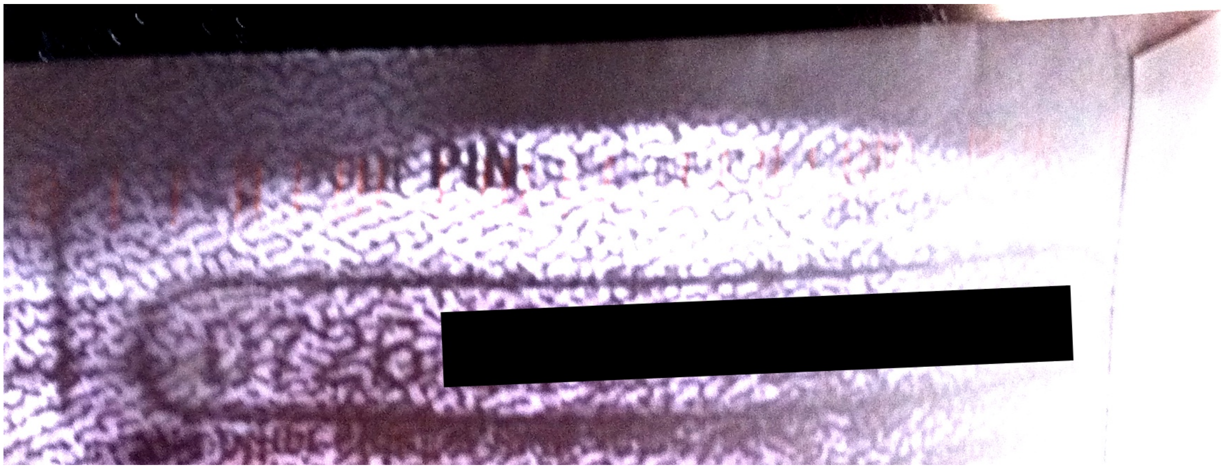
Ultimately, knowledge of a PIN or date of birth does not establish a voter's identity. It merely establishes to the voting server that some entity on the other end of the connection knows a secret. Secrets, of course, can be transferred or intercepted. Indeed, the fraudulent interception of online voting PINs is currently the subject of a criminal investigation in Alberta [7, 19].

Conflict with principles.

This form of voter authentication and eligibility verification may contradict a number of principles. The use of dates of birth evidently contradicts the ballot secrecy principle (see Section 6). The multiple anecdotal accounts of individuals voting on behalf of others would seem to contradict the principles of fairness and eligibility.

4.3 Transparency and Accountability

The opportunity for an independent evaluation of security claims and implementations is vital to the public interest. There are numerous examples in the academic literature of improperly implemented software leading to critical vulnerabilities in online voting technology (see, e.g., [20, 25, 10, 23]).



[redacted]

Figure 1: Voter login credentials visible through mail envelope

As a substantial illustration of this point, academics recently discovered several critical implementation vulnerabilities in Scytl's software as implemented for the proposed Swiss Post national online voting system [15, 17]. These included, among other things, the possibility of the election provider creating a valid-looking mathematical proof of a fake election result. On March 29, 2019, Swiss Post announced that it would suspend its e-voting system as a result of critical "errors in the source code." Importantly, these findings were possible because Swiss Post made the system and source code available for independent review not only to the general public but to the international community (Swiss Post reported 3,200 participants from 137 countries).[17]

No such opportunity for independent review was provided in the election. This fact is troubling, as we found numerous municipal documents in circulation which made security claims which were: short on detail; mostly non-technical; and, largely unverifiable by members of the public.

Result by fiat?

For several months after the election, we received phone calls from council candidates from around the province asking how they could verify the correctness of the online vote totals. Many of them had experienced an unexpected loss, and although they all acknowledged there were entirely legitimate possible explanations for the outcome, they were understandably in search of answers.

Unfortunately, however, there appeared to be little objective evidence either supporting or disputing a particular online election result beyond the clerk's declaration of results itself. None of the deployed online systems produced an accompanying paper trail, and there is currently no online equivalent of risk-limiting audits [18]. [18] nor were any of the deployed systems cryptographic end-to-end verifiable [11].

Based on URLs found in municipal documents obtained under access to information, clerks accessed election results by logging into their vendor's web admin portal, where they could generate reports of events, activity, and results. The extent of objective evidence the clerks received (if any) remains an open question. Many of the public documents we examined either pointed to the existence of an independent

[17] https://www.post.ch/en/about-us/company/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system

[18] We are not aware of a risk-limiting audit ever being performed in an Ontario election, and their legality under the MEA remains an open question.

auditor who performed basic logic and accuracy testing, or to third-party firms who performed routine penetration testing of the online system. Aside from neither of these constituting proof of an election outcome, our search of municipal documents uncovered no publicly available reports on the topic. What reassurance do audits provide the public if their scope, methodology and findings are entirely unavailable?

After the election, several residents and former candidates in Wasaga Beach contacted us to share their deep concern about an unexpected election loss. Among other things, we suggested they inquire as to whether there were any IPs responsible for casting an unusually large proportion of ballots in the election. Initially, residents contacted the vendor but were referred to the city clerk. We then helped them write a freedom of information request. The clerk responded that they could not provide this information because the municipality did not have any such records.

Conflict with principles.

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.

As Elections Ontario pointed out in its study of alternative voting technologies, unless the implementation of an online voting system provides auditable evidence of the election results, then “the process is open to question” [5]. Perhaps the most pressing issue for Ontario municipal elections is whether online voting in the next election can provide candidates an objective measure of certainty in the results they will have worked so hard to achieve.

5 OTHER OBSERVATIONS AND FINDINGS

In this section we present additional election observations and findings.

5.1 Cybersecurity claims

Unsupported security claims can be found throughout the cybersecurity industry. While boasts such as “military-grade encryption” may make for good marketing, it is incumbent upon municipalities to *independently* review security claims made by vendors. There is no such thing as perfect security, so municipalities are cautioned to avoid perpetuating vendor language that uses absolutes and superlatives when discussing a security system.

Throughout our study, we, directly and indirectly, encountered numerous questionable and unsupported security claims made by vendors, councilors, candidates, clerks, and staff. Here are a few examples.

“Our system is completely secure/private”

Regarding security, Simply Voting claims their system is “designed ... to eliminate the risk of electoral fraud.”[19] This claim is particularly troubling in our view, especially given the unsupervised polling environment and absence of any independently verifiable audit mechanism.

[19] https://www.simplyvoting.com/security-and-reliability/

Markham claims Scytl's system "provides an electronic voting platform that has the highest security levels available today."[20] As discussed in Section 4.3, however, a recent public review of Scytl's source code in the Swiss Post system revealed several "critical errors."

Regarding privacy, the West Grey election procedures claim "the names of electors who have voted during the voting period will be provided to the Clerk electronically through the Dominion Voting System. It is not possible to determine how an elector has voted,"[21] and that "no link between voter and votes cast can be established." Similarly, Simply Voting's Security Information Package stated, "it is impossible for municipal staff, Simply Voting employees or any other person to see how you have voted." However our analysis in Section 6 indicates, "impossible" is not an accurate characterization.

"Online voting is more secure than postal vote-by-mail"

The city of Markham commissioned a risk assessment of online voting in 2005, which it has cited with some regularity over the years.[22] Among other findings, the report concluded that vote-by-mail ballot casting carried more than double the risk score of than online voting.[23]

This is an extraordinary claim, and not an assessment widely held among cybersecurity researchers. Instead, the opposite view is generally held, i.e., online voting is *more* risky overall than vote-by-mail, with variation in opinion arising only from the degree to which it is.

The report's conclusion was achieved by applying the OCTAVE method, a "self-directed" methodology. This method was designed to guide an organization through assessing itself. By its own definition and intent, any conclusions derived by this method are subjective and not universally applicable. The report assigned a risk score of 35 for mail-in voting, which it attributed mostly to the perceived risk of accidental threats (i.e., 27.1) and attributes considerably less risk to deliberate/malicious threats (i.e., 7.4). By comparison, the report scores the risk of accidental threats in the online voting setting almost four times lower (i.e., 7.3), while scoring the risk of deliberate threats higher (i.e., 9.4).

Given the 2018 election was shown to have experienced significant disruptions caused by an apparent miscommunication. This threat scenario was not considered by this assessment, suggesting that the actual relative risk, the subjectivity of the methodology notwithstanding, is different from the perceived risk it identifies. Furthermore, the study examines risk entirely in isolation of severity of impact. For example, suppose one was doing a risk assessment of health. In that case, one may conclude that an individual is at a considerably higher risk of catching a cold than developing, say, bone cancer. The impact of the latter relative to the former is so substantial, however, that the relative risk becomes immaterial to the question of whether treating bone cancer should be an important subject of medical research.

By comparison, the US National Institute of Standards and Technology (NIST) performed a threat analysis of ballot return via several modes, including postal mail, phone, fax, e-mail, and web-based [21]. Each threat is categorized across the standard cybersecurity dimensions of confidentiality, integrity, and the system's availability in question. The potential impact of each threat was categorized as being either low,

[20] Award of Proposal 246-R-13. Markham staff report. April 07, 2014. http://www2.markham.ca/markham/ccbs/indexfile/Agendas/2014/General/gc140407/Election%20Report-%20Scan%20Vote%20Tabulation%20and%20Online%20Voting%20System.pdf

[21] West Gray 2018 Municipal Election Procedures. http://www.westgrey.com/public_docs/documents/West%20Grey%20Municipal%20Election%20Procedures%20Revised.pdf

[22] City of Markham. 2018 Municipal Election Information Presentation. March 5, 2017. http://www2.markham.ca/markham/ccbs/indexfile/Agendas/2018/General/gc180305/2018%20Election%20Model%20Presentation.pdf

[23] Henry Kim. Risk Analysis of Traditional, Internet, and other Types of Voting Alternatives for Town of Markham, 2005. http://guelph.ca/wp-content/uploads/RiskAnalysisOfIntenetVoting.pdf

moderate, or high. For ballots returned by postal mail, NIST identified nine threats, of which the impact on confidentiality and integrity were categorized as being either low or moderate. The only threat identified as having a high impact was to availability (a large-scale physical attack on a postal mail-hub). However, such an attack was determined to require high effort and would have a high probability of detection. For ballots returned via the web, NIST identified 17 threats—almost twice as many as postal mail—of which 6 had a high impact on confidentiality, 6 had a high impact on integrity, and 2 had a high impact availability. Each of these threats ranged from low to high effort and low to high in detection probability.

"Our servers use SSL encryption"

The term SSL is widely misused. A modern webserver almost certainly does *not* offer SSL, and it would be inappropriate to do so. SSL ("Secure Sockets Layer") is an outdated and vulnerable network security protocol. It was replaced by TLS ("Transport Layer Security") in 1999, but it was widely supported for the sake of backward compatibility until critical vulnerabilities were discovered in 2015.

Non-technical users will recognize TLS as the padlock icon in a browser's address bar, which denotes a secure network connection with a website. Although TLS provides basic privacy protection via encryption, it performs many other necessary and useful security functions.[24]

We observed many occasions where vendors and municipal staff were confusing the terms SSL and TLS. While there are still legitimate occasions to use the term SSL (e.g., in historical or branding context such as Qualys' SSL Server Test), much of the time people say "SSL" when they mean to say "TLS," and are unaware of the technical difference. For example, Dominion's documentation claimed "the ballot is sent through an encrypted tunnel (SSL) to the application servers."[25]

Our analysis of the network security configurations of the online voting servers used in the 2018 Ontario election, however, found *none* offered SSL (either version 2 or 3).

The use of TLS itself is also unremarkable. On the one hand, TLS represents the primary (and in some cases *only*) line of defense against network-based man-in-the-middle attacks that can steal voter credentials and modify ballot selections. It is such a necessary protection that many web browsers today display an explicit "Not Secure" warning when a user visits a website without it.

On the other hand, TLS is a minimum web security protection, and it would be extraordinary only if an e-voting company *did not* use it. Claiming, as Dominion did, that its servers use "encryption technologies that are proven secure daily by the world's top banks"[26] is unimpressive insofar as *all* banks—and indeed the majority of websites globally—use such encryption technology.[27] Simply Voting claimed "communication between the voter's computer and our website is encrypted with ... strong cipher suites to protect against current and future encryption attacks."[28] Our analysis, however, found Simply Voting servers were offering six weak ciphersuites using non-best practice cryptographic primitives including RSA key exchange, CBC block-cipher modes, and SHA-1 hashing.

[24] Aleksander Essex. 10 Reasons You Need TLS/HTTPS on Your Website. Whisperlab blog post. https://whisperlab.org/blog/2018/Ten-Reasons-You-Need-TLS-HTTPS-on-Your-Website.html

[25] See, e.g., Internet Voting Solution General Security and Operations Overview, Dominion Voting Systems. https://www.midland.ca/Shared%20Documents/Agenda%20-%20General%20Committee%20April%2010.pdf

[26] City of Pickering. 2018 Municipal Elections FAQ. https://www.pickering.ca/en/city-hall/resources/2018-election/Final-Brochure---Residents-August-2018.pdf

[27] https://www.ssllabs.com/ssl-pulse/

[28] Security Information Package, Simply Voting. https://www.stratfordcanada.ca/en/insidecityhall/resources/Elections-2018/Simply-Voting-Security-Information-Package_29Aug18.pdf

This observation's relevance is twofold: in cybersecurity, small details such as a software or protocol version can significantly impact security. In the absence of technical standards or procurement guidance, the difference between secure and insecure software implementations and protocols would not necessarily be evident to municipalities, voters, or, as these examples suggest, even vendors.

"Online banking is secure, therefore online voting is secure"

We heard numerous accounts where the cybersecurity challenges of online banking were being equated to online voting. For example, Cambridge's clerk was quoted in the local paper saying "online voting is no different than banking online."[29]

It cannot be understated the degree to which online voting and online banking are fundamentally different cybersecurity challenges. Municipal councils and staff need to understand that online voting is a subject of fierce international debate. Online voting is *not* like online banking for several important reasons:

- **There is zero secrecy between bank and client.** Your bank requires you to provide detailed information about your identity including your name, address, contact information, social insurance number, employment history, credit history, and even a photograph (via government-issued photo ID). This identity information is *directly* tied to every transaction you ever make, which includes the amount of money you send or receive and the other party's identity. Meanwhile under the principles of the MEA (and indeed any secret ballot election), the association between a voter and their ballot is a *secret*.

- **Fraud is the cost of doing business.** The banking industry remains profitable despite losing billions of dollars to fraud. According to a recent study, the banking industry loses 2.4% of its revenue in fraud claims.[30] Could our democracy tolerate 2.4% of all cast ballots being stolen and modified?

- **Banks closely monitor for unusual activity.** Financial institutions invest heavily in sophisticated fraud prevention and detection techniques. Many of these methods rely on behavioral analysis to classify whether a transaction is normal or suspicious. None of these behavioral methods, however, apply to secret ballot elections. But imagine they were. Suppose you vote for a candidate outside your typical political preference. Later, your phone rings."Hello, we received an alert of unusual activity in your account. We've placed a temporary stop on your ballot. Please contact us at your earliest convenience to confirm your voting intention."

- **Improper charges can be detected and disputed.** If you notice and improper charge, your financial institution has a well-defined process allowing you to submit a claim. The outcome of this claim is something you can track and appeal as necessary. If you were a voter in the 2018 municipal election, ask yourself: what evidence did you receive that your vote was actually counted as intended? How would you find out if it was modified due to fraud or error? How would you dispute it if it was?

[29] Bill Doucet. Cambridge and North Dumfries promote confidence in online voting. Cambridge Times, Oct 6, 2018. https://www.cambridgetimes.ca/news-story/8948329-cambridge-and-north-dumfries-promote-confidence-in-online-voting/

[30] https://www.thestar.com/business/2018/11/21/financial-services-wrestle-with-fighting-rising-fraud.html

- **Remuneration is a remediation.** The remedy for an improper charge is simple: you get your money back. In cases where a company experiences a data breach, you might be offered a free credit monitoring and protection service. Ultimately in a financial setting, remedies are financial in nature. So what is the remedy for a hacked election? Is it as simple as re-running the election? What if the fraud went undetected until *after* the losing party assumed office? As one frustrated Ontario voter suggested to us, perhaps the remuneration for a hacked municipal election should be that you would receive an exemption from one bylaw of your choosing for four years.

- **Banks are heavily regulated.** Banks must conform to strict financial regulations that have precedents dating back hundreds of years. There are federal and provincial bodies dedicated to overseeing the financial industry, and there exist strict penalties to banks for non-compliance. Online voting in Ontario municipalities, however, has not federal or provincial standards governing its use, and little provincial oversight (see Section 3.1)

Ask: how is any of this possible in a secret-ballot election?

"We're confident in the security. We hired a company to do a penetration test"

Penetration testing (also known as *white-hat* hacking) involved paying a cybersecurity company to role-play as malicious cyber-actors. They are invited to conduct reconnaissance and attempt to penetrate the client's systems and servers. They will typically deliver a report and work with the client to address any vulnerabilities discovered during the test. We frequently heard city staff citing penetration testing initiatives as evidence that their system was secure.

While penetration tests for any online voting system should be viewed as necessary, they *cannot* be viewed as sufficient for several important reasons:

- **Generic:** A pentest only looks at general IT threats but doesn't consider application-specific cyber requirements, like ballot secrecy

- **Incomplete:** A pentest does not consider key threat actors like insiders and does not consider voter device security

- **Wrong Emphasis:** A pentest tells you about the technology, but not whether procedures were followed or, importantly, whether the results are correct

- **Non-instructive:** A pentest may tell you about certain cyber-vulnerabilities but doesn't tell you what can go wrong and what to do when it does

- **Secret:** We are not aware of a single municipality making their pentest report publicly available.

A penetration test cannot ensure the security of an online election. Nor should the top-level goal be for staff to convince themselves their election servers are properly configured. It should be to convince the losing candidates that the election results are correct.

5.2 Voter Assistance in an Unsupervised Setting

In remote online, telephone, and postal mail voting, voters cast ballots in an unsupervised environment. Compared to supervised in-person ballot casting, unsupervised voting carries an increased risk that a third party could coercively influence a voter during ballot casting. Voter coercion can arise from a variety of sources seeking to influence or control another's vote. Examples may include a family member in a position of power such as a parent or spouse, or a campaign worker going door-to-door, e.g., with a tablet computer (see e.g., Goodman [13]).

Certain population groups with less experience using computing technology (e.g., residents of retirement communities) can be especially vulnerable to coercion if they require technical assistance in navigating the voting website. The use of online voting technology was at the heart of a court challenge to the election results of Lambton Shores. One of the plaintiffs argued, "we live in a municipality with a significant seniors population, and it was very confusing for them."[31]

We heard several independent anecdotal accounts of the difficulty older voters faced using the online voting website. In particular, the concern was raised about the possibility of candidates running in small towns themselves visiting retirement communities to assist elderly voters.

Municipalities need to know that preventing voter coercion in an unsupervised setting is still an open problem in academic research, and existing approaches pose significant usability and accessibility challenges [11].

5.3 Limitation of Liability

Another critical area for future debate and study is the degree to which an online voting vendor should be held liable for an undermined election. The purpose of this observation is to highlight the current liability arrangements as a starting point to this discussion.

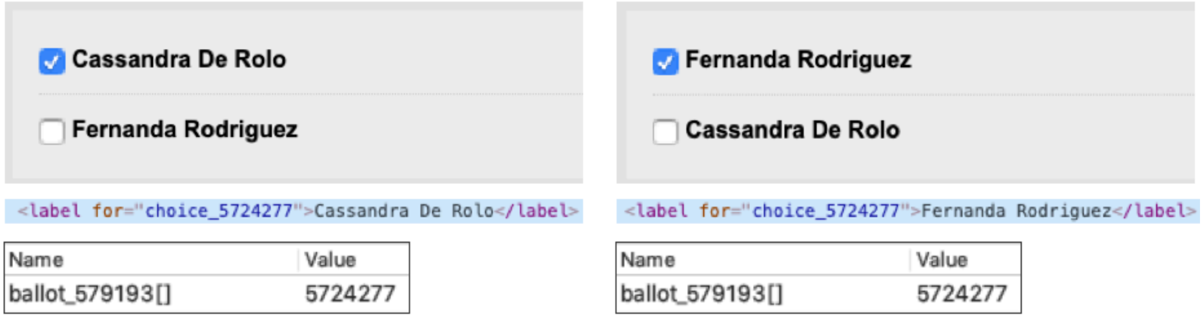
For the most part, the contracts we observed limited the total liability of an online voting vendor to the total amount of the contract. For example, the contract between the town of Cobourg and Intelivote Systems Inc. (ISI) states "the liability for ISI ... shall not exceed the total fee payable to ISI by the Municipality." A similar clause between the city of Cambridge limits Dominion's "total aggregate liability for any loss, damage, costs or expenses under or in connection with this Agreement, howsoever arising, including without limitation, loss, damage, costs or expenses caused by breach of contract, negligence, strict liability, breach of statutory or any other duty shall in no circumstances exceed the total dollar amount of the Agreement."[32]

5.4 Security of Voter Computers

Web-based services usually would not have administrative control over a voters's computer to enforce what code it executes. In each of the vendor systems we examined, the voting client is a Javascript program that runs in the voter's browser. Javascript running in a web browser is *sandboxed*, meaning it is heavily restricted in its ability to interact with, much less control, the overall functioning of a voters' computer outside of the context of the web session it is running in.

[31] Court challenge of Lambton Shores municipal election underway. CTV News. May 31, 2019.https://london.ctvnews.ca/court-challenge-of-lambton-shores-municipal-election-underway-1.4446922

[32] https://www.cambridge.ca/en/elections/resources/17-163.pdf



☑ Cassandra De Rolo

□ Fernanda Rodriguez

```
<label for="choice_5724277">Cassandra De Rolo</label>
```

Name	Value
ballot_579193[]	5724277

☑ Fernanda Rodriguez

□ Cassandra De Rolo

```
<label for="choice_5724277">Fernanda Rodriguez</label>
```

Name	Value
ballot_579193[]	5724277

Figure 2: **Left**: Simply Voting demo site showing a vote cast for De Rolo results in the candidate code 5724277 being sent to the server. **Right**: Demo site with our vote-swapping browser plugin enabled showing a vote cast for candidate Rodriguez *also* resulting in the candidate code 5724277 being sent to the server.

The client (i.e., voter's computer) ultimately has full control over what Javascript executes on their computer, including modifying the code received from the server or arbitrarily modifying responses made to the server. Unlike a paper ballot that shows a voter-made mark directly beside a human-readable name, online voting systems typically represent ballot selections by either a code, id number, or position index, i.e., not the verbatim text of the chosen candidate's name.

As submitted to the election server, this code, id number, or position index representing a voter's ballot preference usually is not accessible to the voter without specialized knowledge of web debugging techniques. If malicious software, such as a malicious browser plugin, could modify the ballot as displayed to the voter while keeping the underlying representation intact, the modification would not be detectable to either the voter or the voting client.

Following the election, a cybersecurity expert in Cambridge Ontario, released a demonstration vote-stealing browser plugin in Chrome.[33] This approach can be used to arbitrarily modify what the voter sees and what actions the browser undertakes. Examples include exfiltrating vote preferences to external servers, modifying buttons, or swapping text lables of candidate names.

We adapted this plug-in to demonstrate vote-swapping on the Simply Voting demo website.[34] Figure 2 demonstrates the vote swapping in action. Simply Voting was the only vendor in the 2018 election to provide a public demonstration website, and therefore the only one we could test.

We also developed and tested an installer script to automatically deploy the plugin on a computer using the Hak5 Rubber Ducky,[35] a small USB device that simulates a keyboard to deliver a scripted sequence of key strokes quickly. Using this device, someone could walk up to a computer and insert it into a USB port and install the plug-in automatically (i.e., without requiring any user interaction) under 10 seconds.

Because none of the existing voting systems were made available to the public for examination, it remains an open question whether any vendor solutions provided any explicit protections against these types of in-browser modification. Dominion claims the ballot is "hash coded (the entire ballot bitmap hash is calculated and appended to the ballot image) to ensure the ballot is not altered by malicious intent before reaching the election servers."[36] This claim seems rather dubious, especially since it appears a ballot can

[33] https://github.com/RawInfoSec/chrome-ext-poc

[34] https://github.com/aleksessex/chrome-vote-swapper

[35] https://shop.hak5.org/products/usb-rubber-ducky-deluxe

[36] Township of Southgate Internet Voting System. January, 2017. https://southgate.civicweb.net/document/83030

be altered *before* any hash is calculated. This same document states London Ontario's Digital Boundary Group carried out a security audit of Dominion's system, but this report is not publicly available to our knowledge (see Section 4.3), and it remains unclear whether this threat was considered.

5.5 Scrutineering in an Online Setting

Scrutineering an online election is fundamentally different in an online setting, and municipalities will need to confront the fact that it may not be democratically meaningful.

One of the roles of a scrutineer is to challenge electors they have reason to believe are ineligible to vote. Given that the online systems used in 2018 accepted ballots based on a remote user entering a valid PIN and date of birth, the ability for a scrutineer to fulfill this role is substantially limited in a remote setting.

Another key role of a scrutineer is to witness the casting and counting of the ballots. We heard several accounts of scrutineers being allowed special access to the system to cast and count dummy ballots. This form of logic & accuracy testing is also limited to the point of being nearly meaningless unless there was some guarantee that any errors or fraud in the main election system would also occur in the test environment to be detectable.

5.6 Data Ownership

Election data ownership appears to be a legal issue that has not been fully explored. For one thing, allowing a municipality to retain ownership over its data does not appear to be a default practice among vendors. One election official told us that they had to "fight" to maintain control of data collected about voters.

The wording of some contracts appears ambiguous. For example, the contract between Intelivote Systems Inc. and Cobourg Ontario (dated May 8th, 2017 and obtained under a freedom of information request) contained the following wording:

> ISI shall maintain ownership of all intellectual property rights associated with the ISI Service, and the Municipality is only entitled to the data concerning the Election generated by the ISI Service, and the Municipality shall have no other rights in or further use of the ISI service.

Another related question is whether a data ownership agreement would include derived information such as statistics. We were sent a report prepared for the town of Wasaga Beach (also obtained under freedom of information) in which Intelivote paired voter demographic data (age, sex, etc.) with meta-information about the election (mode of voting, time of ballot casting, etc.). For example, 78% of women aged 90-99 who voted in the election cast an online ballot. Based on our study we see nothing (at least technologically) that would prevent a vendor from pairing this kind of demographic data with actual ballot selections (e.g., 78% of women aged 90-99 voted for candidate X).

Consider that this kind of information is routinely sold by many large financial institutions, social media and telecom companies. Such companies have data analytics subsidiaries who generate and sell de-identified analytics ("insights") from data gathered by their primary business units' regular operation. For example, there might be a telecom company that collects detailed location data about you through the ordinary course of your cellphone contract and then later sells this information (in aggregate) to a 3rd-party.

It seems to be an open legal question whether such statistics in an aggregated, de-identified state would violate ballot secrecy. At the very least, any municipality using online voting must explore this question.

6 ANALYSIS OF VOTER CONFIDENTIALITY AND BALLOT SECRECY

A significantly overlooked question in the online voting conversation in Ontario has been to what extent an online voting vendor can associate a voter's identity with their ballot selection. Recalling the MEA principle stating secrecy of the ballot is paramount, in this section we ask how unique is a voter's date of birth (DOB) within their particular municipal election.

Data collection.

As part of our study leading up to the election we collected basic web data from each of the 180 active voting websites we found. This included the IP addresses, TLS certificates, HTTP headers, and static HTML of the login pages. We examined the source code of each web page for elements that indicated the presence of a DOB field. In the case of Simply Voting's static HTML login pages, the DOB field was identified by a class definition for the field label (i.e., `<span class="field-label">Date of Birth</span>`). In Intelivote and Scytl's Angular web application, the DOB field was identified as a variable assignment. Dominion's was identified as an HTML list select element. Most voting sites loaded the DOB field dynamically. We did not wish to burden on the election servers by capturing full HTTP sessions of the login pages of every municipality. Loading the login page of a single Dominion municipality, for example, required over 100 separate GET requests, so we opted to capture a single municipality per vendor. As a result do not have a complete accounting of which municipalities used DOB as a login credential, though our sampling of municipal documents suggests a large majority did.

We used a web proxy on the evening of the election to capture HTTP messages sent by the voting client to the election server when the login button was clicked. We used breakpoints so that we could intercept and examine POST messages without actually forwarding them to the server. At the time of capture, we were unable to complete a load of Dominion's login page (see Section 4.1).

We found that within a single web session the server receives information about: the voter's city (from the URL itself), their date of birth (from the login), and how they voted. We now examine the degree to which this information could be used to associate voter and vote.

6.1 Re-identifying Voters with City and Date of Birth

As a rough estimate, there are approximately 30,000 possible dates of birth in a voting age population (365 days times 80 years). Considering that many of the municipalities who ran online voting had voting populations numbering in the low thousands, it seemed likely that many voters would have a unique DOB in their town. To model this, we used the AMO's data on eligible voters in each municipality, combined with a sizable real-world DOB dataset to create a distribution from which we could run experiments to study the uniqueness of dates of birth within each municipality.

Modeling Date of Birth distribution.

Our experiment required a DOB distribution representative of a general population of voting age individuals. In the US, many states provide public access to voter registries. Most include names and postal addresses,

		$k=1$		$k=5$	
Vendor	Eligible Voters	Max Affected	% of Eligible	Max Affected	% of Eligible
Dominion	1,323,194	531,758	(40.2%)	1,181,876	(89.3%)
Intelivote	860,985	613,999	(71.3%)	847,876	(98.5%)
Simply Voting	304,479	190,097	(62.4%)	294,912	(96.9%)
Scytl	253,437	32,880	(13.0%)	123,712	(48.8%)
Total	2,742,095	1,368,734	(49.9%)	2,448,376	(89.3%)

Table 5: Degree to which voters were uniquely identifiable ($k = 1$) or near-uniquely identifiable ($k = 5$) by the use of date of birth as a login credential

and some even include birth dates. We decided to use the statewide Ohio voter registry, which is a large publicly available dataset (>7 million records) containing voter DOB information.[37]

For each municipality, we ran the following experiment: we uniformly sampled dates of birth from the Ohio voter registry equal to the number of eligible voters in the given municipality. To determine the uniqueness of each record, we counted the frequency of each DOB in the sample, and then counted the number of times each frequency value was recorded. The result was a probability distribution of finite outcome, where the probability of each outcome represented the likelihood that a DOB record would have exactly that many matches in the election. We ran 1,000 trials for each municipality, generating a cumulative distribution where the probability of each outcome represented the likelihood that a particular DOB would have up to that many matches in the election. We estimate the number of re-identified voters within a cell size of k by multiplying the number of eligible voters in a given municipality by the probability of k or fewer matches from its cumulative distribution.

Results.

The repeated trial experiment was run for each municipality, determining the maximum number of affected voters that were uniquely identifiable (i.e., $k = 1$). We also considered an *almost* uniquely identifiable case ($k = 5$), which we chose as the smallest cell size found in industry, although a cell size of $k > 20$ is typical. [2]. A breakdown of our findings by vendor is shown in Table 5. Of 9,444,628 eligible voters in the province, 2,742,095 (29.0% of the total voting population) were at some risk of being re-identified by the combination of their city and DOB. Of these, up to 1,368,734 voters (49.9% of the total affected population) could be uniquely identified, and 2,448,376 (89.3% of the total affected population) could be near-uniquely identified. That these numbers are so high is reflective of the fact that much of the 1.4 million voters were spread across numerous small towns, significantly increasing the chance of a unique city/DOB combination. If we were to simulate this effect for the entire province in the scenario where municipalities used online voting, we estimate that up to 2,638,340 voters (27.9%) would be uniquely re-identified and up to 5,302,183 (56.1%) would be near-uniquely identified.

In conclusion, roughly half of the voters eligible to cast online ballots in the 2018 Ontario municipal election were uniquely re-identifiable by their date of birth and town. Given this information is transmitted

[37] Ohio statewide voter files. Available: https://www6.sos.state.oh.us

to the voting server in the same web session as the voter's cast ballot, there is a strong case to be made that dates of birth as login credentials conflicts with the principle of ballot secrecy.

7 RECOMMENDATIONS

Based on this study's findings, we believe the current approach to online voting in Ontario municipalities is unsustainable. The conflict between technology and the democratic and legal principles will lead (and in some cases already has led) to electoral disruptions, legal challenges, and an overall decline in trust and confidence in our democratic institutions.

We agree with the Chief Electoral Officer of Ontario's assessment [6] that:

> As the public becomes more informed about software, malware, and manipulation of technology data systems, they are increasingly interested in knowing exactly how election technology preserves the integrity of our electoral process and the confidentiality of their personal information.

This report goes on to point out that for the public to trust the integrity of the electoral process, they must be assured that:

- Technology used to cast a vote will accurately count the vote as intended.
- Technology used to cast a vote will uphold the secrecy of the vote.
- Technology used to tabulate votes will be verifiable and protected from tampering.
- Technology used to transmit election results will be verifiable and protected from tampering.
- Technology will not result in the breach of their confidential and personal information.

Recommendation 1: Do Not Offer Online Voting Until Standards Are Developed

No technical standards currently exist within Canada for designing, testing, or certifying online voting systems or auditing or otherwise independently verify the result they produce, nor do the federal or provincial governments provide guidance on the procurement and operation of such systems.

In light of the risks, and until cybersecurity standards for online voting can be developed to implement the assurances outlined by Ontario's Chief Electoral Officer, our primary recommendation is that **Ontario municipalities do not offer online voting in the 2022 Municipal election**.

Recommendation 2: Province Should Immediately Begin Standards Development for Online Voting

Based on our study, we believe most municipalities do not have the resources and expertise to assess online voting's technical risk adequately. In a recent survey of Ontario election officials, we found a broad consensus for the idea of standards development of minimum mandatory cybersecurity standards for online voting [12]. Some municipalities have acknowledged that online voting should be deferred until such time as standards can be developed."[38] More recently, the Ontario Chief Electoral Officer has recommended that **Ontario establish common evaluative standards and certification for election technology** [6]. We concur with this recommendation.

Recommendation 3: Update the Municipal Elections Act

The Municipal Elections Act (MEA) no guidance regarding how to deliver an online election. The Ontario Municipal Elections Act addresses online voting only implicitly through the broadly defined notion of "alternative voting methods":

> "The council of a local municipality may pass by-laws ... authorizing electors to use an alternative voting method, such as voting by mail or by telephone, that does not require electors to attend at a voting place in order to vote."[39]

The MEA does not state any principles that would provide a municipality a lens through which to evaluate online voting or any concrete implementation thereof. In contrast to the extensive specification and requirements for paper-ballot voting, the Act makes no mention of online voting or any pertinent fundamental concepts remotely relating to computers, networking, or cybersecurity.

The Act relies on numerous concepts applicable to in-person paper ballot voting with no obvious or immediate analog or equivalent in the online voting context. In certain instances, this appears to lead to a contradiction between the letter of the law and online voting's technological reality. For example, the Act states, "No person shall communicate any information obtained at a voting place about how an elector intends to vote or has voted," (MEA, Sec. 49 (2)c). In fact, the act of casting a ballot in an online voting system communicates–in the literal sense–information about how an elector has voted.

In another example, the Act states, "A candidate may appoint scrutineers to represent him or her during voting and at the counting of votes, including a recount" (MEA, 16(1))." In the circumstance that either a vendor, its sub-contractors, or an agent of the municipality committed a corrupt practice during an online election that altered the election result, an important question is how, or even whether, this would be detectable by the electorate. Given that ballots in the online setting: are cast and counted remotely from the vantage point of the municipality, candidate their scrutineers; are counted using proprietary software on computing systems not otherwise available for inspection by a candidate or their scrutineer, and have no associated paper record, how can a reasonable person conclude scrutinization under such circumstances is in any way meaningful?

We recommend that **the MEA be updated to, at a minimum, acknowledge the existence of online voting.** Preferably, the MEA would also address the fundamental differences between in-person paper ballots and remote online voting. The MEA should also require election results carrying objective evidence of their correctness. To that end, the province should explore risk-limiting audits for optically scanned ballots, and the possibility of cryptographic end-to-end verification (E2E-V) for online ballots.

[38] Waterloo Council Meeting Minutes. November 21, 2016. Available online: https://events.waterloo.ca/meetings/Detail/2016-11-21-1400-Council-Meeting/

[39] Ontario Municipal Elections Act, 1996, S.O. 1996, c. 32, Sched.

Recommendation 4: Province Should Require Municipal Reporting

Currently, no infrastructure, procedure, or precedent exists for CSE, Elections Canada, Elections Ontario, or other cities to share information about emergent threats and vulnerabilities. There is no requirement that a cyber incident is reported to the province. The province does not even track which municipalities use online voting, a task which has so far fallen to private for-profit vendors. As this study revealed, the reported statistics were inaccurate in many cases, and the details were not made public.

We recommend that **Municipal Affairs and Housing track which municipalities use online voting**. Furthermore, we recommend that municipalities be required to report cybersecurity incidents to the province and establish an information-sharing mechanism to alert municipalities to known threats and vulnerabilities.

Recommendation 5: Accept that Public Scrutiny is Both Imperative and Inevitable

The public has a fundamental stake in the security of an online voting system. It is *their* election, and as such, no security claims about online voting can be viewed as being above scrutiny. The opportunity for the independent evaluation of security claims and implementations is vital to the public interest. There are numerous examples in the academic literature of improperly implemented software, leading to critical election technology vulnerabilities.

We recommend that **municipalities be prepared to answer detailed cybersecurity questions from an increasingly informed public**. Municipalities should be prepared for the possibility that information provided to them by their private for-profit online voting vendor is likely insufficient to answer these questions adequately. They should pro-actively seek input from other independent sources, such as other municipalities and organizations (e.g., AMCTO), provincial agencies (e.g., Elections Ontario, Office of the Information and Privacy Commissioner), or other subject matter experts.

Other Recommendations

Recognizing that not all municipalities will be willing to accept Recommendation 1, we have a few interim recommendations that will at least help reduce some of the democratic risks of online voting:

- **Provide Public Evidence of an Election Result.** Do not force losing candidates into a position of having to blindly trust the election results. Commit to providing candidate representatives objective evidence, as is still done in the paper-ballot analog.

- **Be Transparent.** Share security findings with the public and allow them to independently explore vendor security claims via public demonstrations, intrusion tests, or bug bounty programs. Make documentation public, such as source code, system documentation or specifications, penetration testing reports, system auditor reports.

- **Conduct a Privacy Impact Assessment.** Convince yourself and the public that the election vendor cannot link voters with their votes. At the very least, do not make false statements to the contrary.

- **Have a Cyber-Incident Response Plan.** Take the possibility of a network outage seriously and have a contingency plan in place.

- **Require Multi-factor Authentication.** Put up greater barriers to credential sharing among friends and family and be upfront about the unsupervised nature of online voting as it pertains to the possibility of voter coercion.

8 CONCLUSION

There is significant work to be done in Ontario if online voting is to continue in the long term. As one clerk of a large city acknowledged to us, it may take as little as one successful cyber attack for online voting to be banned permanently. The observations made in this study, however, point to a more likely failure mode without hackers, malice, or fraud. Until the technological practice inhabits the same universe as the legal principles, the absence of standards for online voting in Ontario may lead it to collapse on its own.

REFERENCES

[1] *Handbook for the Observation of New Voting Technologies*. Organization for Security and Cooperation in Europe (OSCE) Office for Democratic Institutions and Human Rights, 2013. ISBN 978-92-9234-869-4.

[2] De-identification guidelines for structured data, 2016. Available online: https://www.ipc.on.ca/resource/de-identification-guidelines-for-structured-data.

[3] *Cyber threats to Canada's democratic process*. Canada. Communications Security Establishment (Canada), 2017. Available online: http://publications.gc.ca/site/eng/9.838566/publication.html.

[4] *2019 Update: Cyber threats to Canada's democratic process*. Canada. Communications Security Establishment (Canada), 2019. Available online: http://publications.gc.ca/site/eng/9.872398/publication.html.

[5] *Alternative Voting Technologies Report*. Elections Ontario, 2019. ISSN 978-1-4606-2017-5.

[6] *Modernizing Ontario's Electoral Process: Report on Ontario's 42nd General Election*. Elections Ontario, 2019. Available online: https://www.elections.on.ca/en/resource-centre/reports-and-publications.html.

[7] D. Anderson, C. Dunn, A. Dempster, B. Labby, and A. Neveu. Fraudulent emails used to cast votes in ucp leadership race. *CBC News*, Published April 10th, 2019. Available online: https://www.cbc.ca/news/canada/calgary/ucp-leadership-voter-fraud-membership-lists-data-1.5091952.

[8] N. Boisver. Dead dog registered to cast vote in upcoming mono, ont. election. *CBC News*, Published October 11th, 2018. Available online: https://www.cbc.ca/news/canada/toronto/decease-dog-voting-pin-1.4859489.

[9] C. Butler. Ontario civic elections: the problem with online voting. *CBC News*, April 4th, 2018. Available online: https://www.cbc.ca/news/canada/london/london-ontario-online-voting-1.4598787.

[10] N. Chang-Fong and A. Essex. The cloudier side of cryptographic end-to-end verifiable voting: A security analysis of helios. In *32nd Annual Computer Security Applications Conference (ACSAC '16), CA*, 2016.

[11] S. Dzieduszycka-Suinat, J. Murray, J. Kiniry, D. Zimmerman, D. Wagner, P. Robinson, A. Foltzer, and S. Morina. The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study. US Vote Foundation, 2015.

[12] A. Essex and N. Goodman. Protecting electoral integrity in the digital age: Developing e-voting regulations in canada. In *Election Law Journal: Rules, Politics, and Policy*, volume 19. 2020.

[13] N. Goodman. *Online Voting: A Path Forward for Federal Elections. Report to the Privy Council Office of Canada*. 2017. Available online: https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html.

[14] N. Goodman, J. H. Pammett, and J. DeBardeleben. Internet voting: The canadian municipal experience. 33(3), 2010.

[15] R. Haenni. Swiss post public intrusion test: Undetectable attack against vote integrity and secrecy, 2019. Available online: https://e-voting.bfh.ch/publications/2019/.

[16] J. Laucius. Election night glitch points to the 'wild west' of online voting, says cybersecurity expert. *Ottawa Citizen*, October 25rd, 2019. Available online: https://ottawacitizen.com/news/local-news/election-night-glitch-points-to-the-wild-west-of-online-voting-says-cybersecurity-expert.

[17] S. J. Lewis, O. Pereira, and V. Teague. How not to prove your election outcome. 2019. Available online: https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf.

[18] M. Lindeman and P. B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 10(5):42–49, 2012.

[19] A. MacVicar. Alberta ndp calls for special prosecutor to oversee rcmp investigation of ucp leadership race. *Global News*, Published May 2nd, 2019. Available online: https://globalnews.ca/news/5233913/notley-special-prosecutor-ucp-leadership-race/, May 2019.

[20] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas. The return of coppersmith's attack: Practical factorization of widely used rsa moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1631–1648. ACM, 2017.

[21] A. Regenscheid and N. Hastings. *A Threat Analysis on UOCAVA Voting Systems*. Number NISTIR 7551. US National Institute of Standards and Technology, 2008.

[22] F. Scarpaleggia et al. *Strengthening Democracy in Canada: Principles, Process and Public Engagement for Electoral Reform*. Canada. Parliament. House of Commons. Special Committee on Electoral Reform, 2016. Available online: http://publications.gc.ca/site/eng/9.828533/publication.html.

[23] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. 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.

[24] M. Warren. Online voting causes headaches in 51 ontario cities and town. *Toronto Star*. Published October 23rd, 2019. Available online: https://www.thestar.com/news/gta/2018/10/23/internet-voting-causes-headaches-in-51-ontario-cities-and-towns.html.

[25] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. *Financial Cryptography*, chapter Attacking the Washington, D.C. Internet Voting System, pages 114–128. 2012.

A 2018 ONLINE VOTING USE BY MUNICIPALITY

Municipality	Total Eligible Voters	Vendor Name (If Online Voting Offered)	24-hour Emergency Voting Extension?	Same-night Emergency Voting Extension?
Addington Highlands, Township of	4,586	Intelivote		
Adelaide-Metcalfe, Township of	2,415	Intelivote		
Adjala-Tosorontio, Township of	8,719			
Admaston/Bromley, Township of	2,965			
Ajax, Town of	77,885	Simply Voting		
Alberton, Township of	702			
Alfred and Plantagenet, Township of	8,149	Intelivote		
Algonquin Highlands, Township of	3,361			
Alnwick/Haldimand, Township of	6,385	Intelivote		
Amaranth, Township of	3,385	Intelivote		
Amherstburg, Town of	17,324			
Armour, Township of	2,247			
Armstrong, Township of	815			
Arnprior, Town of	6,420	Intelivote		
Arran-Elderslie, Municipality of	5,037			
Ashfield-Colborne-Wawanosh, Township of	5,786	Simply Voting		
Asphodel-Norwood, Township of	3,401	Simply Voting		
Assiginack, Township of	1,594			
Athens, Township of	2,622			
Atikokan, Town of	2,185			
Augusta, Township of	5,962	Intelivote		
Aurora, Town of	38,935	Dominion		
Aylmer, Town of	5,081	Intelivote		
Baldwin, Township of	648			
Bancroft, Town of	3,579			
Barrie, City of	92,156			
Bayham, Municipality of	5,167			
Beckwith, Township of	6,512			
Belleville, City of	34,592	Dominion		
Billings, Township of	1,512			
Black River-Matheson, Township of	2,702			
Blandford-Blenheim, Township of	5,948			
Blind River, Town of	3,127			
Bluewater, Municipality of	8,768	Simply Voting		
Bonfield, Township of	1,839			
Bonnechere Valley, Township of	4,101			
Bracebridge, Town of	15,000	Dominion	●	
Bradford West Gwillimbury, Town of	23,808	Dominion	●	
Brampton, City of	313,273			

Brant, County of	26,571			
Brantford, City of	66,619	Dominion		●
Brethour, Township of	Acclaimed			
Brighton, Municipality of	9,094			
Brock, Township of	10,042			
Brockton, Municipality of	7,712	Dominion	●	
Brockville, City of	15,600	Intelivote		
Brooke-Alvinston, Municipality of	2,055			
Bruce, County of	Upper-tier			
Bruce Mines, Town of	529			
Brudenell, Lyndoch and Raglan, Township of	2,293			
Burk’s Falls, Village of	719			
Burlington, City of	128,238	Dominion		
Burpee and Mills, Township of	Acclaimed			
Caledon, Town of	51,192			
Callander, Municipality of	3,412			
Calvin, Municipality of	622			
Cambridge, City of	87,750	Dominion		●
Carleton Place, Town of	7,819	Intelivote		
Carling, Township of	3,193	Intelivote		
Carlow/Mayo, Township of	693	Intelivote		
Casey, Township of	Acclaimed			
Casselman, Village of	2,847	Intelivote		
Cavan Monaghan, Township of	7,278	Simply Voting		
Central Elgin, Municipality of	10,717			
Central Frontenac, Township of	7,345	Intelivote		
Central Huron, Municipality of	7,082	Simply Voting		
Central Manitoulin, Municipality of	3,168			
Centre Hastings, Municipality of	4,040	Intelivote		
Centre Wellington, Township of	20,266	Intelivote		
Chamberlain, Township of	Acclaimed			
Champlain, Township of	7,340	Intelivote		
Chapleau, Township of	1,694			
Chapple, Township of	727			
Charlton and Dack, Municipality of	Acclaimed			
Chatham-Kent, Municipality of	76,418	Dominion		
Chatsworth, Township of	5,964			
Chisholm, Township of	Acclaimed			
Clarence-Rockland, City of	17,600	Intelivote		
Clarington, Municipality of	65,373			
Clearview, Township of	12,117	Intelivote		
Cobalt, Town of	929			
Cobourg, Town of	14,700	Intelivote		
Cochrane, Town of	4,224			

Cockburn Island, Township of	Acclaimed			
Coleman, Township of	825			
Collingwood, Town of	19,713	Dominion	●	
Conmee, Township of	727			
Cornwall, City of	32,912			
Cramahe, Township of	5,254			
Dawn-Euphemia, Township of	1,887			
Dawson, Township of	657			
Deep River, Town of	3,239	Simply Voting		
Deseronto, Town of	1,225			
Dorion, Township of	Acclaimed			
Douro-Dummer, Township of	6,819	Simply Voting		
Drummond/North Elmsley, Township of	7,001			
Dryden, City of	5,372	Simply Voting		
Dubreuilville, Township of	474			
Dufferin, County of	Upper-tier			
Durham, Regional Municipality of	Upper-tier			
Dutton/Dunwich, Municipality of	3,265			
Dysart, et al., United Townships of	13,526			
Ear Falls, Township of	772			
East Ferris, Township of	4,463			
East Garafraxa, Township of	Acclaimed			
East Gwillimbury, Town of	19,568			
East Hawkesbury, Township of	Acclaimed			
East Zorra-Tavistock, Township of	4,800	Intelivote		
Edwardsburgh/Cardinal, Township of	5,044	Intelivote		
Elgin, County of	Upper-tier			
Elizabethtown-Kitley, Township of	8,325	Intelivote		
Elliot Lake, City of	9,529			
Emo, Township of	1,018			
Englehart, Town of	1,121			
Enniskillen, Township of	Acclaimed			
Erin, Town of	8,685			
Espanola, Town of	3,838			
Essa, Township of	13,086			
Essex, County of	Upper-tier			
Essex, Town of	15,417			
Evanturel, Township of	Acclaimed			
Faraday, Township of	2,504			
Fauquier-Strickland, Township of	618			
Fort Erie, Town of	23,559			
Fort Frances, Town of	5,286	Intelivote		
French River, Municipality of	4,049			
Front of Yonge, Township of	2,378			

Frontenac Islands, Township of	2,190	Intelivote		
Frontenac, County of	Upper-tier			
Gananoque, Town of	3,558	Intelivote		
Gauthier, Township of	141			
Georgian Bay, Township of	9,533	Dominion	●	
Georgian Bluffs, Township of	10,195	Dominion	●	
Georgina, Town of	33,844			
Gillies, Township of	530			
Goderich, Town of	6,343	Simply Voting		
Gordon/Barrie Island, Municipality of	Acclaimed			
Gore Bay, Town of	Acclaimed			
Grand Valley, Town of	2,663	Intelivote		
Gravenhurst, Town of	13,692	Dominion	●	
Greater Madawaska, Township of	4,915	Simply Voting		
Greater Napanee, Town of	12,094	Intelivote		
Greater Sudbury, City of	115,784	Dominion	●	
Greenstone, Municipality of	3,510	Intelivote		
Grey Highlands, Municipality of	9,887	Dominion	●	
Grey, County of	Upper-tier			
Grimsby, Town of	20,560	Simply Voting		
Guelph, City of	93,650			
Guelph/Eramosa, Township of	9,979			
Haldimand County	36,820			
Haliburton, County of	Upper-tier			
Halton Hills, Town of	43,203			
Halton, Regional Municipality of	Upper-tier			
Hamilton, City of	363,434			
Hamilton, Township of	9,055	Intelivote		
Hanover, Town of	5,411	Dominion	●	
Harley, Township of	Acclaimed			
Harris, Township of	Acclaimed			
Hastings Highlands, Municipality of	7,036	Intelivote		
Hastings, County of	Upper-tier			
Havelock-Belmont-Methuen, Township of	7,255	Simply Voting		
Hawkesbury, Town of	8,365	Intelivote		
Head, Clara and Maria, Township of	614			
Hearst, Town of	3,790			
Highlands East, Municipality of	8,851			
Hilliard, Township of	208			
Hilton Beach, Village of	229			
Hilton, Township of	Acclaimed			
Hornepayne, Township of	822			
Horton, Township of	2,760			
Howick, Township of	2,995	Simply Voting		

Hudson, Township of	574			
Huntsville, Town of	18,277	Dominion	●	
Huron East, Municipality of	7,022	Simply Voting		
Huron Shores, Municipality of	2,331			
Huron-Kinloss, Township of	7,158	Dominion	●	
Huron, County of	Upper-tier			
Ignace, Township of	1,031			
Ingersoll, Town of	9,285			
Innisfil, Town of	27,904	Dominion	●	
Iroquois Falls, Town of	3,701			
James, Township of	432			
Jocelyn, Township of	813			
Johnson, Township of	861			
Joly, Township of	658			
Kapuskasing, Town of	6,391			
Kawartha Lakes, City of	66,441	Dominion	●	
Kearney, Town of	2,441			
Kenora, City of	10,676	Simply Voting		
Kerns, Township of	Acclaimed			
Killaloe, Hagarty and Richards, Township of	3,111			
Killarney, Municipality of	1,302	Intelivote		
Kincardine, Municipality of	9,802	Dominion	●	
King, Township of	16,976			
Kingston, City of	82,950	Dominion		●
Kingsville, Town of	15,118			
Kirkland Lake, Town of	6,010			
Kitchener, City of	152,238			
La Vallee, Township of	753			
Laird, Township of	1,150			
Lake of Bays, Township of	8,079	Dominion	●	
Lake of the Woods, Township of	633			
Lakeshore, Town of	27,356			
Lambton Shores, Municipality of	10,904	Intelivote		
Lambton, County of	Upper-tier			
Lanark Highlands, Township of	6,781	Intelivote		
Lanark, County of	Upper-tier			
Larder Lake, Township of	1,025			
LaSalle, Town of	23,342	Intelivote		
Latchford, Town of	436			
Laurentian Hills, Town of	2,396			
Laurentian Valley, Township of	7,722	Dominion	●	
Leamington, Municipality of	16,309	Intelivote		
Leeds and Grenville, United Counties of	Upper-tier			
Leeds and the Thousand Islands, Township of	9,818	Intelivote		

Lennox and Addington, County of	Upper-tier			
Limerick, Township of	1,018	Intelivote		
Lincoln, Town of	17,005	Dominion		
London, City of	248,212			
Loyalist, Township of	12,129	Intelivote		
Lucan Biddulph, Township of	3,533	Intelivote		
Macdonald et al., Township of	1,704			
Machar, Township of	1,781			
Machin, Township of	936			
Madawaska Valley, Township of	5,642			
Madoc, Township of	1,988			
Magnetawan, Municipality of	3,627			
Malahide, Township of	5,910			
Manitouwadge, Township of	1,634			
Mapleton, Township of	6,762			
Marathon, Town of	2,467			
Markham, City of	196,689	Scytl		
Markstay-Warren, Municipality of	2,445			
Marmora and Lake, Municipality of	4,803	Intelivote		
Matachewan, Township of	435			
Mattawa, Town of	1,599			
Mattawan, Township of	Acclaimed			
Mattice-Val Cot, Township of	695			
McDougall, Township of	3,652	Intelivote		
McGarry, Township of	641			
McKellar, Township of	3,044	Intelivote		
McMurrich/Monteith, Township of	1,737			
McNab/Braeside, Township of	6,181	Intelivote		
Meaford, Municipality of	10,309	Dominion	●	
Melancthon, Township of	2,444	Intelivote		
Merrickville-Wolford, Village of	2,708	Intelivote		
Middlesex Centre, Municipality of	12,152	Intelivote		
Middlesex, County of	Upper-tier			
Midland, Town of	13,200			
Milton, Town of	62,521			
Minden Hills, Township of	11,392	Intelivote		
Minto, Town of	6,275			
Mississauga, City of	442,649			
Mississippi Mills, Municipality of	10,704	Intelivote		
Mono, Town of	7,180	Intelivote		
Montague, Township of	3,100	Intelivote		
Moonbeam, Township of	1,597			
Moosonee, Town of	983			
Morley, Township of	Acclaimed			

Morris-Turnberry, Municipality of	2,897	Simply Voting		
Mulmur, Township of	3,492	Intelivote		
Muskoka Lakes, Township of	17,006	Dominion	●	
Muskoka, District Municipality of	Upper-tier			
Nairn and Hyman, Township of	575			
Neebing, Municipality of	2,569			
New Tecumseth, Town of	26,856			
Newbury, Village of	Acclaimed			
Newmarket, Town of	56,748	Scytl		
Niagara Falls, City of	61,859			
Niagara-on-the-Lake, Town of	14,213			
Niagara, Regional Municipality of	Upper-tier			
Nipigon, Township of	1,030			
Nipissing, Township of	2,737			
Norfolk County	49,266			
North Algona Wilberforce, Township of	3,412			
North Bay, City of	37,272			
North Dumfries, Township of	7,742	Intelivote		
North Dundas, Township of	8,380	Intelivote		
North Frontenac, Township of	Acclaimed			
North Glengarry, Township of	8,099	Intelivote		
North Grenville, Municipality of	12,650	Intelivote		
North Huron, Township of	3,852	Simply Voting		
North Kawartha, Township of	6,762	Simply Voting		
North Middlesex, Municipality of	4,837	Intelivote		
North Perth, Municipality of	9,687			
North Stormont, Township of	5,242	Intelivote		
Northeastern Manitoulin and The Islands, Town of	3,281			
Northern Bruce Peninsula, Municipality of	9,644	Dominion	●	
Northumberland, County of	Upper-tier			
Norwich, Township of	7,737			
O’Connor, Township of	619			
Oakville, Town of	125,936			
Oil Springs, Village of	532	Intelivote		
Oliver Paipoonge, Municipality of	4,984			
Opasatika, Township of	227			
Orangeville, Town of	20,321			
Orillia, City of	23,766			
Oro-Medonte, Township of	18,175	Dominion	●	
Oshawa, City of	108,138			
Otonabee-South Monaghan, Township of	5,828	Simply Voting		
Ottawa, City of	633,946			
Owen Sound, City of	15,257	Dominion	●	
Oxford, County of	Upper-tier			

Papineau-Cameron, Township of	1,121			
Parry Sound, Town of	4,960	Intelivote		
Peel, Regional Municipality of	Upper-tier			
Pelee, Township of	483			
Pelham, Town of	14,264			
Pembroke, City of	9,579	Dominion	●	
Penetanguishene, Town of	6,802	Dominion	●	
Perry, Township of	2,900			
Perth East, Township of	8,271	Simply Voting		
Perth South, Township of	3,079			
Perth, County of	Upper-tier			
Perth, Town of	4,590	Intelivote		
Petawawa, Town of	12,929	Dominion	●	
Peterborough, City of	58,022	Dominion		●
Peterborough, County of	Upper-tier			
Petrolia, Town of	4,229	Intelivote		
Pickering, City of	67,748	Dominion		●
Pickle Lake, Township of	305			
Plummer Additional, Township of	922			
Plympton-Wyoming, Town of	6,901	Intelivote		
Point Edward, Village of	1,600	Intelivote		
Port Colborne, City of	15,240			
Port Hope, Municipality of	12,984	Intelivote		
Powassan, Municipality of	2,839			
Prescott and Russell, United Counties of	Upper-tier			
Prescott, Town of	3,216	Intelivote		
Prince Edward, County of	21,975	Dominion		●
Prince, Township of	Acclaimed			
Puslinch, Township of	5,742			
Quinte West, City of	30,899	Dominion		
Rainy River, Town of	644			
Ramara, Township of	11,146	Intelivote		
Red Lake, Municipality of	2,829	Simply Voting		
Red Rock, Township of	740			
Renfrew, County of	Upper-tier			
Renfrew, Town of	6,070	Dominion	●	
Richmond Hill, Town of	114,000			
Rideau Lakes, Township of	12,435	Intelivote		
Russell, Township of	12,655	Intelivote		
Ryerson, Township of	1,190			
Sables-Spanish Rivers, Township of	3,212			
Sarnia, City of	53,151	Intelivote		
Saugeen Shores, Town of	12,252	Dominion	●	
Sault Ste. Marie, City of	55,261			

Schreiber, Township of	981			
Scugog, Township of	17,296			
Seguin, Township of	9,109	Intelivote		
Selwyn, Township of	15,890	Simply Voting		
Severn, Township of	13,747			
Shelburne, Town of	4,876	Intelivote		
Shuniah, Municipality of	3,855	Intelivote		
Simcoe, County of	Upper-tier			
Sioux Lookout, Municipality of	3,200	Simply Voting		
Sioux Narrows-Nestor Falls, Township of	995			
Smiths Falls, Town of	6,498	Intelivote		
Smooth Rock Falls, Town of	1,024			
South Algonquin, Township of	636			
South Bruce Peninsula, Town of	12,489			
South Bruce, Municipality of	4,685	Dominion	●	
South Dundas, Municipality of	7,834	Intelivote		
South Frontenac, Township of	17,606	Intelivote		
South Glengarry, Township of	10,088	Intelivote		
South Huron, Municipality of	7,516	Simply Voting		
South River, Village of	812			
South Stormont, Township of	10,336	Intelivote		
South-West Oxford, Township of	5,645	Intelivote		
Southgate, Township of	5,852	Dominion	●	
Southwest Middlesex, Municipality of	4,236	Intelivote		
Southwold, Township of	3,562			
Spanish, Town of	755			
Springwater, Township of	15,895	Dominion	●	
St. Catharines, City of	92,226			
St. Clair, Township of	11,648			
St. Joseph, Township of	1,557			
St. Marys, Town of	5,364			
St. Thomas, City of	27,477	Simply Voting		
St.-Charles, Municipality of	1,760			
Stirling-Rawdon, Township of	3,949			
Stone Mills, Township of	6,757	Intelivote		
Stormont, Dundas and Glengarry, United Counties of	Upper-tier			
Stratford, City of	23,478	Simply Voting		
Strathroy-Caradoc, Municipality of	16,243	Intelivote		
Strong, Township of	2,031			
Sundridge, Village of	939			
Tarbutt, Township of	652			
Tay Valley, Township of	6,900	Intelivote		
Tay, Township of	9,441			
Tecumseh, Town of	18,779	Intelivote		

Tehkummah, Township of	730			
Temagami, Municipality of	2,059			
Temiskaming Shores, City of	7,766			
Terrace Bay, Township of	1,201			
Thames Centre, Municipality of	9,979	Intelivote		
The Archipelago, Township of	5,130	Intelivote		
The Blue Mountains, Town of	12,066	Dominion	●	
The Nation Municipality	9,792	Intelivote		
The North Shore, Township of	921			
Thessalon, Town of	1,170			
Thornloe, Village of	79			
Thorold, City of	14,471			
Thunder Bay, City of	81,135	Intelivote		
Tillsonburg, Town of	12,339	Intelivote		
Timmins, City of	30,248	Dominion		●
Tiny, Township of	18,496			
Toronto, City of	1,880,371			
Trent Hills, Municipality of	11,918	Intelivote		
Trent Lakes, Municipality of	11,083	Simply Voting		
Tudor and Cashel, Township of	1,670	Intelivote		
Tweed, Municipality of	5,728	Intelivote		
Tyendinaga, Township of	3,371			
Uxbridge, Township of	16,459			
Val Rita-Harty, Township of	683			
Vaughan, City of	201,488			
Wainfleet, Township of	5,929			
Warwick, Township of	2,717	Intelivote		
Wasaga Beach, Town of	21,874	Intelivote		
Waterloo, City of	72,598			
Waterloo, Regional Municipality of	Upper-tier			
Wawa, Municipality of	2,131	Intelivote		
Welland, City of	38,362			
Wellesley, Township of	7,714	Dominion	●	
Wellington North, Township of	8,124			
Wellington, County of	Upper-tier			
West Elgin, Municipality of	4,931	Intelivote		
West Grey, Municipality of	10,941	Dominion	●	
West Lincoln, Township of	11,651			
West Nipissing, Municipality of	12,150			
West Perth, Municipality of	6,773	Dominion		●
Westport, Village of	628			
Whitby, Town of	90,099			
Whitchurch-Stouffville, Town of	30,025			
White River, Township of	698			

Whitestone, Municipality of	3,673	Intelivote		
Whitewater Region, Township of	6,344	Dominion	●	
Wilmot, Township of	15,919			
Windsor, City of	150,602			
Wollaston, Township of	2,541			
Woodstock, City of	29,678			
Woolwich, Township of	17,384	Dominion	●	
York, Regional Municipality of	Upper-tier			
Zorra, Township of	6,174			

B MUNICIPALITIES DECLARING EMERGENCY VOTING EXTENSIONS

On election night, Dominion issued a press release (see Appendix C) stated “approximately 51” municipalities were affected by the bandwidth slowdown. Our analysis found this number was actually 43 (of 49 municipal clients). To our knowledge our list is the only one to have been made publicly available.

No change to voting period:

Aurora, Belleville, Burlington, Chatham Kent, Lincoln, Quinte West.

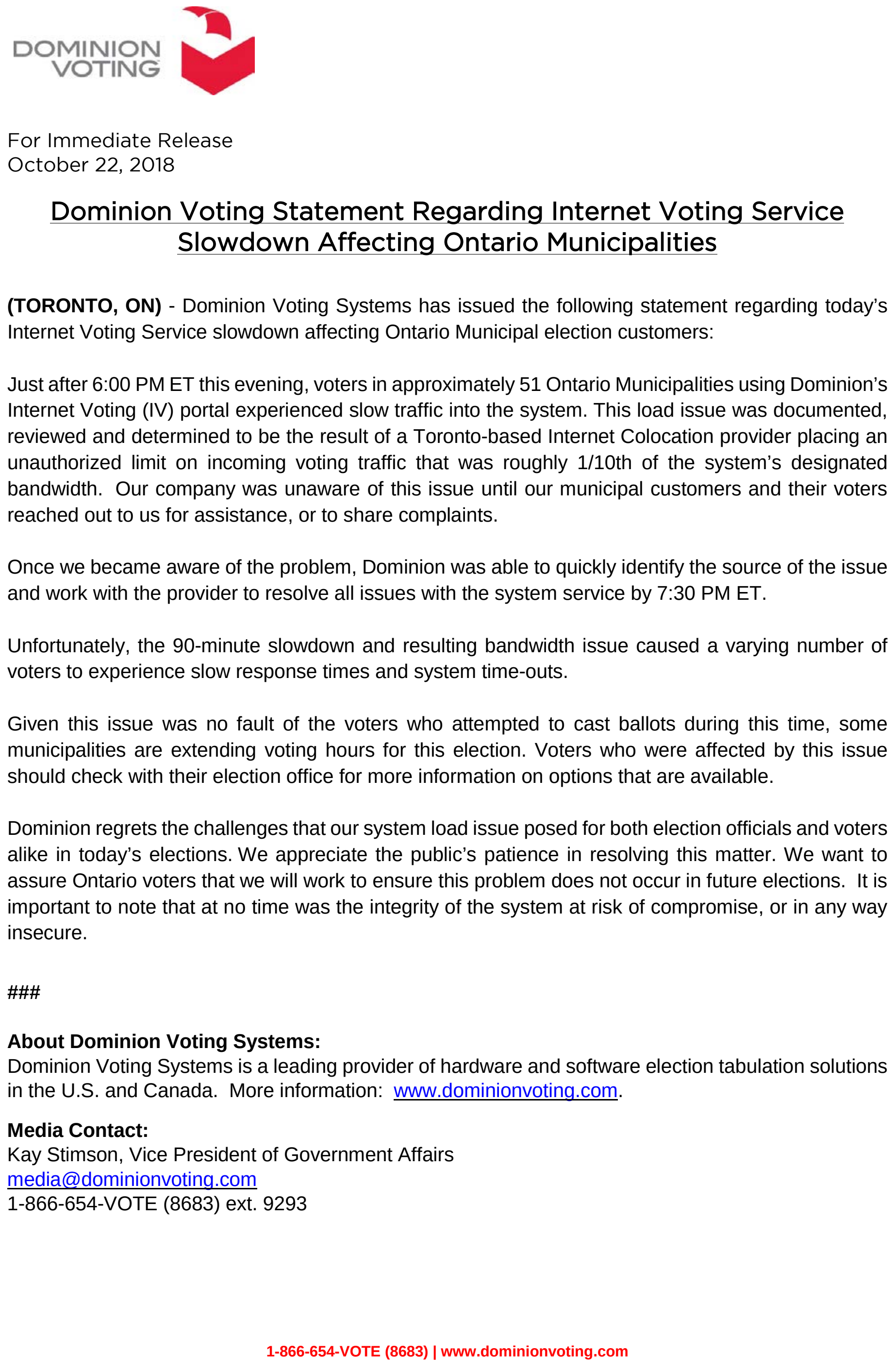
Same-evening extension to voting period:

Brantford, Cambridge, Kingston, Peterborough, Pickering, Prince Edward County, Timmins, West Perth.

24-hour extension to voting period:

Bracebridge, Bradford West Gwillimbury, Brockton, Collingwood, Georgian Bay, Georgian Bluffs, Gravenhurst, Greater Sudbury, Grey Highlands, Hanover, Huntsville, Huron Kinloss, Innisfil, Kawartha Lakes, Kincardine, Lake of Bays, Laurentian Valley, Meaford, Muskoka Lakes, Northern Bruce Peninsula, Oro-Medonte, Owen Sound, Pembroke, Penetanguishene, Petawawa, Renfrew, Saugeen Shores, South Bruce, Southgate, Springwater, The Blue Mountains, Wellesley, West Grey, Whitewater Region, Woolwich.

C DOMINION'S ELECTION NIGHT STATEMENT



For Immediate Release
October 22, 2018

Dominion Voting Statement Regarding Internet Voting Service Slowdown Affecting Ontario Municipalities

(TORONTO, ON) - Dominion Voting Systems has issued the following statement regarding today's Internet Voting Service slowdown affecting Ontario Municipal election customers:

Just after 6:00 PM ET this evening, voters in approximately 51 Ontario Municipalities using Dominion's Internet Voting (IV) portal experienced slow traffic into the system. This load issue was documented, reviewed and determined to be the result of a Toronto-based Internet Colocation provider placing an unauthorized limit on incoming voting traffic that was roughly 1/10th of the system's designated bandwidth. Our company was unaware of this issue until our municipal customers and their voters reached out to us for assistance, or to share complaints.

Once we became aware of the problem, Dominion was able to quickly identify the source of the issue and work with the provider to resolve all issues with the system service by 7:30 PM ET.

Unfortunately, the 90-minute slowdown and resulting bandwidth issue caused a varying number of voters to experience slow response times and system time-outs.

Given this issue was no fault of the voters who attempted to cast ballots during this time, some municipalities are extending voting hours for this election. Voters who were affected by this issue should check with their election office for more information on options that are available.

Dominion regrets the challenges that our system load issue posed for both election officials and voters alike in today's elections. We appreciate the public's patience in resolving this matter. We want to assure Ontario voters that we will work to ensure this problem does not occur in future elections. It is important to note that at no time was the integrity of the system at risk of compromise, or in any way insecure.

###

About Dominion Voting Systems:
Dominion Voting Systems is a leading provider of hardware and software election tabulation solutions in the U.S. and Canada. More information: www.dominionvoting.com.

Media Contact:
Kay Stimson, Vice President of Government Affairs
media@dominionvoting.com
1-866-654-VOTE (8683) ext. 9293