Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?*

Anthony Cardillo[1], Nicholas Akinyokun[2], and Aleksander Essex[1]

[1]Department of Electrical and Computer Engineering
Western University, London, ON, Canada
{acardill,aessex}@uwo.ca

[2]School of Computing and Information Systems
The University of Melbourne, Australia
oakinyokun@student.unimelb.edu.au

Abstract. This paper presents the first comprehensive study of the use of online voting technology in the province of Ontario, Canada. Despite having one of the largest concentrations of online voters globally, its use is not governed by any federal or provincial standards. This has left many municipalities to make decisions largely in isolation, relying on for-profit vendors to set their own bar for cybersecurity and public accountability. This study presents important observations about online voting use in the 2018 Ontario municipal election and questions whether the legal principles are being met by the technology deployed in practice.

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]

* This paper is an extended abstract. The full version is available online: `https://whisperlab.org/ontario-online.pdf`

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

In this paper, 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 [5].

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.

Contribution. We present the first comprehensive study of the cybersecurity of online voting in Ontario's 2018 municipal elections, including a complete accounting of municipalities, ballot options, vendor partnerships, and the extent of municipalities affected by emergency extensions to the voting period on election night. We present findings showing issues with weak voter authentication; poor transparency 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. We study date of birth as a login credential and show that it could by used to uniquely re-identify up to 50% of online voters in the 2018 election.

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 [18, 3].

2.1 Online Voting in Ontario Municipalities

Municipalities in the provinces of Ontario and Nova Scotia have held online elections since 2003 [10]. Since then, adoption in Ontario has followed an exponential

trend, nearly doubling with each election cycle. As 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. [17]). 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.

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

[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`

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.

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.

[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`

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 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

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

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 (`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.

In terms of the correctness of self-declared vendor figures, we observed three of the four vendors reporting more municipal clients than actual elections run. See the full report for further discussion.

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.

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

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.

Of those, 177 offered an online voting option, of which 131 were completely paperless. Our full dataset is available for download online.[8]

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.[9]

We observed 4 vendors active in the 2018 Ontario election: Dominion Voting Systems, Intelivote Systems, Simply Voting, and Scytl. 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 mailing 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.

4 Election Observations and Findings

In this section we present three significant findings. Additional findings are presented in the full version.

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

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

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.

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 [8]. 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 [20, 12].

A statement by Dominion 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." 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 the full version.

Five months after the election we were invited to present preliminary results of this paper to the Association of Municipal Managers, Clerks and Treasurers

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

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. According to Sudbury's post-election report, however, the slowdown was determined to be a "miscommunication between Dominion and the service provider."[10]

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 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 [7].

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.

[10] 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`

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

The use of single credential for voter authentication is inadvisable since access to the voter information 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 5), 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 [6, 15].

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 5). The multiple anecdotal accounts of individuals voting on behalf of others would seem to contradict the principles of fairness and eligibility.

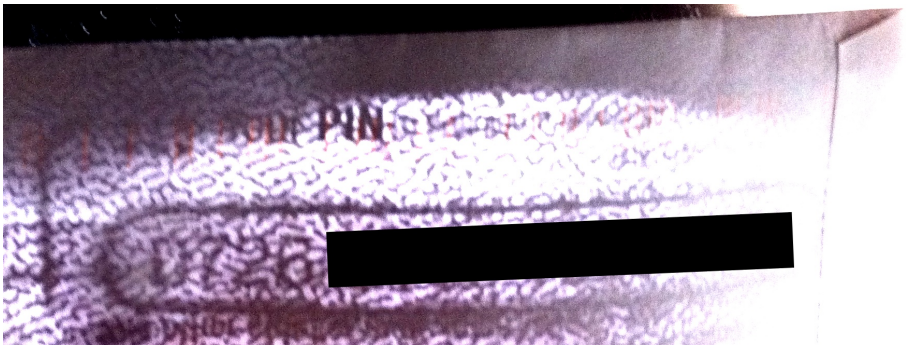

Fig. 1. Voter login credentials visible through mail envelope

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., [16, 21, 9, 19]).

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 [11, 13]. 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).[11]

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

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

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 [14].

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 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" [4]. 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 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 in-

cluded 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. 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.

5.1 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, 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.[12]

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

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

		$k=1$		$k=5$	
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

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 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.

6 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.

Acknowledgments. We are grateful to a many individuals in Ontario and beyond for important insights on technology, policy and law. Special thanks to Jane Buchanan. See the full version of the complete list of acknowledgments.

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

[5] *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`.

[6] 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`.

[7] 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`.

[8] 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`.

[9] 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.

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

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

[12] 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`.

[13] 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`.

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

[15] 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.

[16] 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.

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

[18] 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`.

[19] 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.

[20] 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`.

[21] 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.