City Council
Meeting Agenda

Consolidated as of April 21, 2017

April 24, 2017 – 6:00 p.m.
Council Chambers, Guelph City Hall, 1 Carden Street

Please turn off or place on non-audible all electronic devices during the meeting.

Please note that an electronic version of this agenda is available on guelph.ca/agendas.

Authority to move into closed meeting

That the Council of the City of Guelph now hold a meeting that is closed to the public, pursuant to the Municipal Act, to consider:

Confirmation of minutes for the closed Council meeting held on March 27, 2017.

C-CON-2017.7 **ATU Collective Bargaining Mandate Request**
Section 239 (2) (d) labour relations or employee negotiations.

Open Meeting – 6:30 p.m.

O Canada
Silent Reflection
First Nations Acknowledgement
Disclosure of Pecuniary Interest and General Nature Thereof

Closed Meeting Summary

Confirmation of Minutes: (Councillor Gibson)

That the minutes of the open Council Meetings held March 27 and April 10, 2017, and the open meeting minutes of the April 3, 2017 Committee of the Whole, be confirmed as recorded and without being read.

Committee of the Whole Consent Report:

The following resolutions have been prepared to facilitate Council's consideration of various matters and are suggested for consideration. If Council wishes to address a specific report in isolation of the Committee of the Whole Consent Report, please identify the item. It will be extracted and dealt with separately as part of the Items for Discussion.

COW-PS-2017.02 Outstanding Resolutions of Public Services

Recommendation:

That the recommendations marked as "completed" within Report# PS-17-05 Outstanding Resolutions of Public Services be removed from the outstanding resolutions list.

COW-PS-2017.03 Animal Control By-law Chicken Amendments

Recommendation:

1. That as detailed in Public Services Report #PS-17-04 Animal Control By-law chicken amendments, that staff be directed to create an amendment to the Animal Control By-law (2016)-20122 to permit residents that cannot facilitate a 15 metre (50 feet) distance for the keeping of poultry to keep chickens provided the following can be met:

   Hen coops and hen runs shall be a distance of at least 1.2m from the rear lot line and at least 1.2m from any side lot line of the dwelling lot on which the hen coop is located (meeting the setback requirements as per the zoning bylaw);

   Pens (includes hen coop and hen run) must be located the furthest from any other dwelling, and must be 1.2m away from any property line;

   Pens shall be located at least 7.5m from the lot line to any religious institution or business or school;

   Pens shall be a minimum distance of 3m from all windows and doors of dwellings that are located on an abutting property;

   Pens are not permitted in any front or side yard;

   That the maximum number of hens be limited to ten (10).

2. That as detailed in Public Services Report #PS-17-04 Animal Control By-law chicken amendments, that staff be directed to create an amendment to the Animal Control Bylaw (2016)-20122 requiring food for poultry be stored in an animal proof secured container.

3. That as detailed in Public Services Report #PS-17-04 Animal Control By-law chicken amendments, that staff be directed to create an amendment to the Animal Control By-law (2016)-20122 requiring that coop floors be lined with an appropriate material to absorb fecal matter and to facilitate cleaning.

4. That as detailed in Public Services Report #PS-17-04 Animal Control By-law chicken amendments, that staff be directed to create an amendment to the Animal Control By-law (2016)-20122 requiring that residents keeping backyard chickens shall provide each hen with food, water, shelter, light, ventilation, appropriate substrate flooring, and provide opportunities for essential behaviours such as scratching, nesting, including but not limited to dust-bathing, and roosting, to maintain each hen in good health and welfare.

5. That as detailed in Public Services Report #PS-17-04 Animal Control By-law chicken amendments, that staff be directed to create an amendment to the Animal Control By-law (2016)-20122 prohibiting persons from killing a domestic animal on their property, except by a licenced vet or otherwise authorized by the City of Guelph.

COW-CS-2017.02 Tax Ratios 2017-2020 Assessment Cycle

Recommendation:

1. That the Tax Ratios for the 2017 year be adopted as set out in Table One of the "Tax Ratios 2017-2020 Assessment Cycle" Report CS-2017-02 dated Monday, April 3, 2017.

2. That the Tax Ratios for the remainder of the 2017-2020 assessment cycle be adopted based on start ratios for all tax classes except for the multi-residential ratio which will remain revenue neutral on an annual basis.

3. That the tax ratios be incorporated into the appropriate Tax Policy.

COW-CS-2017.03 2017 Tax Policy

Recommendation:

1. That the 2017 City of Guelph Property Tax Policies set out in Schedule 1 to the "2017 Tax Policy" CS-2017-07 report dated April 3, 2017, be approved.

2. That the tax policies be incorporated into tax ratio, tax rate, and capping by-laws to be adopted on April 24, 2017.

3. That a tax rate related to the dedicated infrastructure levy be calculated for the required amount and identified separately on the 2017 and future years' City tax bills replacing the previously separated Public Health levy.

4. That the maximum allowed capping parameters be used for 2017, allowing the City of Guelph to exit the capping program in the shortest time frame available.

COW-2017.01 Councillors Mike Salisbury and Leanne Piper Request for Access to Additional Training Funding 2017

Recommendation:

That Councillor Leanne Piper be authorized to exceed her 2017 training allocation of $3250 to an upset limit of $400 in order to attend the American Planning Association conference in May 2017.

CON-2017.09 Surplus Asset Sales Policies – Mayor Guthrie's Motion for which notice was given on March 6, 2017

Recommendation:

1. That staff report back on the City of Guelph's policy on local community non-profit access to surplus assets through our Wellbeing Grant policy.

2. That staff be directed to facilitate the potential transfer of one surplus ambulance to St. John's Ambulance within the 2017 budget from the Infrastructure Renewal Reserve.

Council Consent Agenda:

The following resolutions have been prepared to facilitate Council's consideration of various matters and are suggested for consideration. If Council wishes to address a specific report in isolation of the Consent Agenda, please identify the item. It will be extracted and dealt with separately as part of the Items for Discussion.

CON-2017.11 Habitat for Humanity Development Charge Late Payment Agreement

Recommendation:

That the Mayor and Clerk be directed to execute the Development Charge late payment agreement with Habitat for Humanity, generally in the form included as Attachment 2 to IDE Report 17-46, dated April 24, 2017.

Items for Discussion:

The following items have been extracted from the Committee of the Whole Consent Report and the Council Consent Agenda and will be considered separately. These items have been extracted either at the request of a member of Council or because they include a presentation and/or delegations.

CON-2017.14 Annual Report from the Integrity Commissioner

Presentation:
Robert Swayze, City of Guelph Integrity Commissioner

Recommendation:

That the 2016 Annual Report of the Integrity Commissioner, dated April 24, 2017, be received.

CON-2017.12 Nomination of a City of Guelph Representative to Apply for a Federation of Canadian Municipalities (FCM) Board of Director Position

(staff memo)

Recommendation:

1. That Council endorse _____________ to stand for election on the Federation of Canadian Municipalities (FCM) National Board of Directors (Ontario Chapter) for the period starting in June 2017 and ending June 2018.

2. That Council confirms it will assume all costs associated with the representative's attendance at FCM's Board of Directors meetings and Annual Conference.

COW-CS-2017.04 2018 Municipal Election: Methods of Voting

(staff memo)

Delegations:

Anne Gajerski-Cauley
Aleksander Essex
Brian Holstein
George Kelly
Dave Suffling
Cameron Shelley
Jason Dodge and Brad Howcroft
Bill McLellan
Susan Watson
Ron East
Lin Grist
Dennis Galon
Maggie Laidlaw
Hugh Whiteley
Laura Root

Correspondence:

Richard Chaloner
Jared Ferrall
Eric Unger
Shawna Cartwright
Bob Moore
Susan Watson (additional submission)
Terry Robins
Jenn Kentner
Ray Stultz
Leah Scott
Todd Billings
Kevin Cahill
Tina Bonesso
Thomas Mooney
Stephanie Scapinello
Laura Roy
Aaron and Janice Douma
Bob Speaker
Nick Porcellato
Steve and Marlene Truscott
Victor McQuade
Lianne Keais
Rachel Schenk
Alex Barr
Cantrys Rondeau
Dan Tourangeau
Lindsay Smith
Jeff and Jen Cummings
Krystal Nicholson
Colleen Morrow
Tania Archbold
Lynette Churchill
Bryanne Aubrey
Marcia Barrett-Chatrand
Laurie Armstrong

Justin Van Daele
Ian Bier
Beverly-Ann Woods
Don McLellan
Eric Rapaci
Joel Croft
Ryan and Kelly Gerritsen
Jane Martin
Marg Harbin
Ferne Pederson
Chris Cates (additional submission)
Jeremy Nicholls
Joe Longo
Michael Reichlmayr
Elke Ruthig
Neil Rocha
Brendon Carson
Angela Clayson
Patrick Ireland
Sarah Rodrigues
Dolly and Ran Kambo
Alex Boughen
Dave Wilkinson
Amy MacIntyre
Hugh Martin
Louis Marchesano
Rishabh Naik
Kim Andrews
Suresh Naik
Mike Willis
Stuart Burke
Debbie Bush
Ryan Laurie
Matthew Wilson
Ian Kitchener
Kelly Zago
Donna and Steve Dodge
Mike Baker
Kara Perez
Thomas Miller
Tom Wiltsie and Jen McDermott
Vera Martin
Christina Tourangeau
Andrew Wellwood
Ron Ramsay
Lisa Natarelli
Laura Zver
Nathan Drescher

Rena Akerman
Michael Smyth
Lisa Buck
Bev Smyth
Brandon Raco
Denise Fell
Andrea Campbell Smith
Alan Jarvis
Terrie Jarvis
Wendy Dabbs
Adam MacIntyre
Sylvia Thurston
Colleen McElwain
Andrea Finlay
Dawn Humphrey
Brenda and Ian Walton
Melina Finnigan
Scott and Kimi Corney
Peter McCaskell
Michael Doyle
DE Harvey
Don Pflug
Andrew Friend
Carolan Sorbara
Jane Darch
Martha Jakowlew
Doug Minett
Robert White
Matthew Brunsting
Rob Brown
Liz Lindsay
Ryan Truscott
Alexandra Whate
Jane Londerville
Jane Aubrey
Helen Daniecki
George Allan
Terri Brown
Treena Adhikari
Sean and Shainna Poulin
Susan Carey
Sean Alexander
Melissa Bortolon
Peter Revie
Nancy Revie
Sabrina Circelli
Darina Griffin
Tony Meekes

Kelly Alves
Ze’ev Gedalof
Katerina Drescher
Ryan Fitzsimmons
Dave Estill
Scott McGregor
Katherine Hitch
Nick Scott
Erin Branson
Terry Wheeler
Dave Collins
Stacey Anne
Jamie Strickland
Brooks Hipgrave
Enzo Fonte
Rebecca Kingshott
Ron Peters
Tom Redman
Dan Freeman
Doug MacMillan
Wendy Banks
Wally Harris
Alison Davidson
Mark Paralovos
Erin Stuart
Michael Stultz
Kristen Chiasson
Steve Van Dam
John Scott
Chris Dawso
Patrick Stiles
Duy Nguyen
Ted Pritchard
Pat Matisz
Arni Mikelsons
Cameron Shelley
Claudette Young
Linda Kearns
Dale and Freda Murray
Pete and Anita Van Rootselaar
Julie Bowman
Françoise Py-MacBeth
David Rekker
Bree Woods
Sam Dent
Judy Dezell
Paul Peteranac
Shawn Johnson
Geof Kearns
Glen Wilson
Elizabeth Snell
Sandy Nicholls
Sally Ludwig
Tony Leighton
Tom Klein Beernink
Russ Peebles
Michael Keefer
Karen Phipps
Dave Withers
Gail Costigan
Richard Akerman
Elizabeth Macrae
Margaret Carter
Andrew Seagram
Glenna Fryer
Inderjit Arora
Ben McCarl
Marlene Pfaff
Jennifer Sumner
Marsaye Treen
Robert Routledge
David Josephy
Derek Kinsman
Dennis Galon
Steve Mercer
Charlene Dwyer
Mark Kenny
Heather Burke
Meg Thorburn
Amy Skeoch
Kris Kenney
Gary Roberts
Kayla McKay
Sabrina Moore
Barry Smith
Devinder Ghuman
Les Indoe
Katie Henderson
Gary Langdon
Jenn Ephgrave
Michael Chumbley
Roxanne Eszes
Stacey Roberts
Jesse Clark
Miki Grosz
Maria Berardine

Jennifer McFadden
Leanne Stultz
Laurie Garbutt
Daniel Bell
Jane Rodd
Susan Moziar
John Cunningham
Norm Bazinet
Monique ten Kortenaar
Jane Moore
Trevor Favaro
Stacy Cooper
Jason Rice
Mark Berardine
Ashley Richardson
Kelli Rice
Scot Barlow
Sarah Parro
Cheryl Sajkowski
Ken Chase
Deby Smith
Yves Younan
Sam Turton
Shelly Martin-Ganson
Jim Rooney
Charlie Cares
Karen Sweigard
Evan Ferrari
Chantal Lapointe
Jackie Speers
Theresa Barras
Kelly McCullough
Patrick Stevens
Mark Kidd
Kelly Caldwell
Andy Saunders
Lynda Murray
Nigel Brown
Kevin Librach
Tammy LaPierre Thompson
Carlie Roberts
Kiran Raj Pandey
Amy Wright
Michelle Wood
Amanda van de Pol
Matt Peters
Jason Inglis
Susan Merritt
Rob Green
Kate Marentette
Ataharul Chowdhury
Laura Root
Lana Haines
Dennis Gray
John Parkyn
Vincent and Kimberley Rogers
Julie Horrocks
Dave Kaczorowski
Margaret Carter
Norman Liota
Aleksander Essex
Cameron Shelley
Brad Howcroft and Jason Dodge

Recommendation:

That a By-law be adopted to support the use of vote scanners/tabulators in the 2018 Municipal Election.

Special Resolutions

CON-2017.15 Exploring Pathways for Aligning Guelph's Corporate Assets with the Low Carbon Economy

1. That the following motion be referred to the Committee of the Whole for consideration:

That in alignment with the CEP mandate, city staff, in coordination with the newly formed Climate Change Office be directed to explore pathways for transitioning the corporation to net zero, or similar, low carbon designation.

That staff examine the current fleet procurement policy and explore pathways to fully electrifying the corporations transportation fleet.

That staff report back on potential next steps in Q4 of 2017.

CON-2017.16 Notice of Motion Policy

1. That the following be referred to the May 1, 2017 Committee of the Whole:

   That Council suspend the use of Notices of Motion until staff bring forward a clear policy on their purpose and intent.

By-laws

Resolution to adopt the By-laws (Councillor Gordon).

"That By-law Numbers (2017)-20160 to (2017)-20169, inclusive, are hereby passed."

By-law Number (2017)-20160	A by-law to authorize the execution of a Engineering Services Agreement between Terra View Custom Homes Ltd., Terra View Construction Ltd. and The Corporation of the City of Guelph. (Harts Village Subdivision)
By-law Number (2017)-20161	A by-law to authorize the execution of a Professional Consulting Services Agreement between Terra View Custom Homes Ltd., Terra View Construction Ltd. and The Corporation of the City of Guelph. (Harts Village Subdivision)
By-law Number (2017)-20162	A by-law to remove Part Lot Control from Lots 10 to 20 inclusive, lots 27 to 35 inclusive, lots 41 and 42, Plan 61M214 designated as Parts 1 to 44 inclusive, Reference Plan 61R21061in the City of Guelph. (multiple addresses on Ambrous Crescent and Kirvan Drive)

By-law Number (2017)-20163	A By-law to authorize alternative methods of voting for the 2018 Municipal Election.
By-law Number (2017)-20164	A by-law to set tax ratios and tax rate reductions for prescribed property subclasses for the Corporation of the City of Guelph for the year 2017.
By-law Number (2017)–20166	A by-law to levy education tax rates for the year 2017.
By-law Number (2017)–20167	A by-law to impose and levy a rate of taxation for the Board of Management for the Downtown Business Improvement Area of the City of Guelph for the 2017 taxation Year.
By-law Number (2017)-20168	A by-law to set the tax rates for City purposes for the year 2017 and to provide for a final tax levy and he payment of taxes.
By-law Number (2017)-20169	A by-law to confirm the proceedings of the meeting of Guelph City Council held April 10 and 24, 2017.

Mayor’s Announcements

Please provide any announcements, to the Mayor in writing, by 12 noon on the day of the Council meeting.

Notice of Motion

Adjournment

INTERNAL MEMO

DATE	Tuesday April 18, 2017
TO	**Clerks**
FROM	Cathy Kennedy
DIVISION	CAO’s Office
DEPARTMENT	Intergovernmental Relations, Policy & Open Government
SUBJECT	**Amendment to April 24, 2017 Council Report – FCM Nomination**

With respect to Report Number CAO-I-1704 (Nomination of a City of Guelph Representative to Apply for a Federation of Canadian Municipalities (FCM) Board of Director Position), please remove recommendation #1 and replace it with the following recommendation:

That Council endorse ____________ to stand for election on the Federation of Canadian Municipalities (FCM) National Board of Directors (Ontario Chapter) for the period starting in June 2017 and ending June 2018.

The modification is intended to provide greater clarity to the recommendation as a stand-alone statement.

Thank you.

Cathy Kennedy
Manager, Policy and Intergovernmental Relations
Intergovernmental Relations, Policy & Open Government

T 519-822-1260 x 2255
E cathy.kennedy@guelph.ca

MEMO

DATE April 24, 2017

TO **City Council**

FROM Stephen O’Brien, City Clerk and Returning Officer

DEPARTMENT City Clerk’s Office

SUBJECT **Clarification of Election Voting Methods Information**

Committee of the Whole was presented with the 2018 Municipal Election: Methods of Voting report on April 3, 2017. During discussions at that meeting, questions were asked by members of Council and information was presented by delegates. This memo is intended to provide additional information and clarification regarding questions raised at and after the April 3, 2017 meeting.

Internet Security and Privacy

TECHNICAL

Procurement and Procedures
The City requires security measures to be in place to secure the information that is cast in an online ballot and, simultaneously, protect the privacy of electors casting their vote. As a rule, this means that information is encrypted, the transfer of information is to a dedicated server, there is no trace back to the elector once the ballot is cast and there are measures in place to prohibit changing of the vote or people multiple voting.

Security requirements for the internet voting system, include, but are not limited to, the following security and privacy requirements:

- Data processing methods to detect and report errors and provide correction messages to the voter (i.e. an incomplete mandatory field).
- HTTPS protocol requirements - confirms that a secured link is being used.
- Secure sockets layer (SSL) being the standard security protocol for establishing an encrypted link between a web server and a browser. This link ensures that data passed between the web server and browsers remain private and secure.
- Ensuring clear and evident separation of registration and authentication procedures and casting/transfer of the vote.
- Securing identification and authentication of the voter and integration with the City's voters’ list to ensure that one ballot is cast per each validated individual (automatic strike off, through secure encrypted transmission of information).
- The two-step voting process requires a validation of human interface such as a challenge that requires the voter to type a series of letters which appear in a picture, including an accessible option of the challenge.
- The system shall verify the authenticity of the ballot and prevent modification of the vote after the ballot is cast, and no record of the vote shall be saved on the voter’s computer.
- Transmission of the ballot, along with a timestamp and voter’s ID, to the vote server in an encrypted form and severed in order to protect the privacy and integrity of the information and prevent the voter from being linked to how they voted.
- The system shall not allow recording or caching of voter transaction if voter is using a public machine to access a ballot, and no ability to perform a screen

printout or capture the screen to a file.

- Encryption of information transmitted between the voter's browser and the election server and protection of data on interfaces between vendor systems and the City of Guelph.
- IP addresses used to record the vote are monitored in order to audit patterns that could imply voting irregularities.
- Intrusion detection systems shall be in place to ensure no hacking and to identify and advise of any suspicious voting activity, which prevents a distributed denial of service (DDOS) attack in which multiple compromised computer systems attack a target. Security practices include performing ongoing security assessments to identify and resolve vulnerabilities, using network security controls, email phishing testing and proactive network monitoring.

In addition, security and privacy requirements are embedded in the City's election procedures in the following ways:

- At the completion of the logic and accuracy testing, the entire voting system is locked down prior to the start of the advanced voting period. No system, code or configuration changes can occur during the lock down or once voting has started.
- The internet voting system is hosted by the internet service provider within their own data center environment which undergoes continuous and rigorous penetration prevention testing. An offsite backup data center in another city is also used to ensure redundancy in case of a prolonged power outage or an equipment failure.
- The internet voting system prevents the casting of multiple ballots via the internet and/or at a voting location. Once a voter PIN is used to cast a ballot, it is flagged by the system and the voter is immediately struck off of the live electronic voters' list. This ensures that an eligible voter cannot obtain another ballot online or at a voting location at any time.
- Once a voter presses the "cast ballot" button in the internet voting system and their ballot is received, the system prevents any modification to the ballot through strict system security and access controls. The confirmed cast ballot screen does not show which candidates the voter selected and the ballot selections are not stored or cached on the voter's computer. Once a voter submits their ballot, they will not be able to re-access or view their selections. No voter data, session ID or selections are stored on the voter's computer or device.
- At the time a ballot is cast, the internet voting system records the action in their database, an audit record is created and an image of the ballot is captured with a timestamp to ensure that there are multiple ways to verify that no votes have been modified. The system will also capture unique identifiers, such as IP addresses, which are never connected to personally identifiable information, and are used for the sole purpose of monitoring for suspicious activities.
- If at any time during the internet voting process there is a disruption of service, the system times out, or a voter closes their browser before the "cast ballot" button is selected, the registered internet voter may re-enter the system and continue the voting process. When they re-enter the system the voter will receive a new blank ballot to resume their voting and any previous selections will be removed to ensure the privacy and security of voting. No information on their previous selections are stored locally on their device or by the internet voting system.

- Once the voter selects the "cast ballot" button, the voter is stuck off the voters' list and any information identifying the voter is separated from the ballot information as soon as the ballot is cast. The ballot information is encrypted directly after the vote is submitted and cannot be decrypted until Election Officials initiate the tabulation and reporting process at the end of voting day.
- As the ballot is submitted, the communication between the web browser and the internet voting provider's servers is digitally signed and encrypted to protect from any external access to or tampering with the ballot.
- Once internet voting is complete, the ballot results data can only be accessed from a secure administrative internet voting website with a login provided to the City Clerk or designated Election Official. The encrypted data file is then transferred to the results reporting system.
- During the results retrieval process, all actions, successful or unsuccessful, are logged and auditable by the system. Unlike paper ballot processes, internet voting processes are auditable before, during and after voting concludes.

Third Party Audit
In 2014, the City joined a group of municipalities in conducting a third party security and threat assessment audit of the internet voting system. The other municipalities involved in this group included the City of Peterborough, Prince Edward County, City of Belleville, Municipality of Port Hope, Municipality of Chatham-Kent, City of Burlington, City of Kingston, and the City of Cambridge. This testing was conducted in August and early September 2014 to allow time to conduct the test and, if any issues were found, to allow sufficient time for correction and follow up testing. The security audit involved the following steps:

a) Information Gathering **-** The testing team collected as much information as possible about the target application. This involved accessing the application to gain a better understanding of the application's logic and identifying where application entry points reside.

b) Enumeration **-** The testing team extracted as much information as possible about each component that makes up the web-based application. This information is gathered through the use of various tools and procedures including but not limited to:

    a. Determining all accessible services and their associated software versions through port scanning and application fingerprinting.
    b. Manual crawling of the application to see if the application or running services may be accessed with commonly known login credentials, to identify how the application handles errors or unexpected input, and to locate any files that are unreferenced such as backup or sample files in order to check for information leakage.
    c. Vulnerability scanners are used to test for numerous application vulnerabilities as well as potential deficiencies with the installation, configuration or management of the application or its associated host system(s).

c) Research **-** From the data gathered in the information gathering and enumeration phase the testing team identified how vulnerabilities can be exposed and exploited.

d) Exploitation **-** Various techniques were used to exploit the vulnerabilities that have been identified in prior phases, such as brute force attacks or exploitation of known software bugs.

The City received a report on the results of the steps outlined above. This report included a technical review, key findings and implications, a prioritized list of action items to address any vulnerabilities identified. Findings of the audit were brought to the City's internet voting system provider and any areas identified were addressed and resolved prior to the beginning of internet voting. A similar third party security and threat assessment audit would be implemented in advance of the 2018 municipal election should internet voting be authorized by Council.

Privacy of the Vote
The system does collect the IP address of the elector who voted. Once the vote is cast the IP address and the vote are separated, and there is no way of knowing how the elector at that IP address voted. Further there is no way of knowing who the person was who used that IP address.

NON-TECHNICAL

Integrity of the Voters' List
Once the Preliminary List of Electors (PLE) is received from the Municipal Property Assessment Corporation (MPAC), the City Clerk and designated election officials review the list to ensure that duplications and inaccuracies are corrected. MPAC draws information from a property database, that is also used for the purposes of calculating municipal taxation, and an additional names database. The information municipalities are provided with includes name, address, ward and poll, birthdate and school support, gender, residency and occupancy status, and citizenship.

When people move, even within the City, they can still be on the list at their previous address. This may be due to many reasons, including: the timing of their move; incomplete information on their new property form; or, they may have moved from being owners to tenants. The list is property owner based and, as such, tenant information is not easily captured. MPAC does provide tools through which land owners can verify and update their tenant information.

Given that municipal elections occur every 4 years, on-campus students are not kept on the list between elections.

List management consists of making the requested changes to the list from applications received and also cleansing the list. Cleansing involves reviewing name anomalies, street anomalies, duplicate electors (people who may own one or more properties or live at one and own another, or moved within city), and incomplete information (i.e. first name only, incomplete birthdate), and deleting information which is incomplete or duplicate; and, correcting information for consistency.

Once under the authority of the City, voters' list changes are also made to the list through submission of a revision form or process which includes identification.

Revisions to the Voters' List

The Municipal Elections Act (MEA) allows a person to add, remove or make changes to their own information or apply to remove a deceased person. The application to add, remove or make changes must be in writing and filed either in person, by mail or in any format and manner that the City Clerk specifies.

At the City of Guelph, revisions to the list require a hard copy or electronic form to be completed and filed with the City Clerk, in person, by mail or electronically. In each case, the City requires a person to show identification, being the same prescribed proof of identity and residence as required to vote at the polling location. An application to add, remove, (other than removal of deceased), or change another person’s information is not permitted.

In addition to being able to remove a deceased person through an application form to the City Clerk and pursuant to section 25 of the MEA, the City Clerk may, on his or her own initiative, remove a person’s name from the voters’ list if satisfied that the person has died. Since 2014, deaths have been verified against information provided to and by the Provincial Office of the Registrar General which enhances the voters’ list.

Voter Cards

Individual voter cards, which contain information on where to vote and how to vote online, are sent in sealed envelopes to each elector with their name appearing on it. Voter cards contain a bar code which allows staff at voting locations to strike people off the list and an ID number for the purpose of registering to vote online. Each person at an address receives an individual sealed voter card.

Two-Step Registration to Vote Online

Electors require their ID, name, address, and birthdate, and email address in order to register to vote. The birthdate is used because there is a need to rely on information provided on the MPAC list. At that time, each individual also provides an answer to a question, which can be used if the elector has issues accessing their ballot. Election staff use all the preceding information to verify who the individual is if they are having difficulty with online voting. Once the registration is complete, a PIN is sent to the elector’s email, which is also required in order to vote.

Verification of Internet Vote

Once a ballot is cast and the results are reported, election staff do not question electors regarding their vote. To do so would be to question the integrity of the vote and, without cause to do so, may result in unwarranted concern. If there are any irregularities of voting noted by the system, the City Clerk’s Office would be apprised and would seek appropriate recourse and, where necessary, pursue enforcement and prosecution.

Voting Online

In order to vote an elector requires a voter ID number and a PIN. In order to ensure that it is not a machine intending to vote, a human interface task or “captcha” is required. Electors are also required to confirm that they are the elector they say they are, and that they understand the corrupt practices notice, which is the same as that which is posted on the voting screens at voting locations. This confirmation is done through the requirement to have online voters acknowledge they have read and understand the associated notices.

Online Voting Assistance

Electors are able to call or email the election office for assistance, if they are having difficulty voting. Elections staff verifies the identity of the elector by name, address and birthdate, and also by asking the question they originally answered when registering.

Election Procedures for Institutions and Retirement Homes

In the City of Guelph, as per Section 45 of the MEA, we provide on-site voting on Election Day at retirement homes with 50 beds or more and institutions with 20 beds or more. We attend bedside or anywhere within the facility for the purpose of voting.

The legislation does not require municipalities to attend to private residences. The legislation also does not preclude municipalities from doing so, however staff do have concerns in relation to the resourcing required to carry out such processes.

Internet Accessibility

It should be noted that the Ontario Human Rights Commission states that the "electoral principle of accessibility recognizes persons with disabilities should be able to vote without assistance." Although many people view accommodations for people with physical limitations as meeting accessibility requirements, there are disabilities which are not physical in nature and which may also prevent people from attending voting locations. As such, these individuals would be more enfranchised through the ability to cast their vote via the internet.

The internet voting registration system and the voting process has the ability to be read by screen readers.

The internet voting provider has developed the system using standardized HTML and JavaScript. The system functions with common assistive technology software including screen readers, screen magnification software, voice dictation software, and onscreen keyboards. The online voting system would be required to be compliant with WCAG 2.0 Level AA guidelines, which meet requirements of the *Accessibility for Ontarians with Disabilities Act*.

The internet voting process allows:

- An independent voting channel
- An audio component for human verification (CAPTCHA)
- 24/7 opportunity to vote for a prolonged period for great convenience
- Ability to vote from any location in the world with internet access

Following the 2014 Election, staff have had several electors comment that it was the first time they were able to vote independently without having to be accompanied by another person at the voting location and/or behind a voting screen.

Proving Identity when Voting

There has been discussion regarding requirements in the provision of identification prior to receiving a ballot and the differences in this regard between in-person and online voting. Section 52 of the MEA states that a person entering a voting place shall be provided a ballot if the person presents the prescribed proof of identity OR if they complete a form stating they are the person on the voters' list.

Similarly, an internet voter is required to confirm, by checking off a box that they are the elector, named on the list. In addition the internet voter must confirm that they have read and are aware of corrupt practices and offences as listed under the MEA. This same document is posted on voting screens at polling locations, but electors at voting locations are not required to verify that they have read and understood them.

Recount

There has been discussion about the necessity of having a paper trail of a voter's intention to vote and that the City has, in recent years, been required to conduct a full manual recount.

Section 60(1) of the MEA states that a recount under shall be conducted in the same manner as the original count, whether manually or by vote-counting equipment.

There has been discussion which implies that there has been a manual ballot poll tabulator recount in a past recount. In 2014, there was a recount which was conducted in ward 3. The ballots were fed through the tabulators as they were originally and the internet results were uploaded to the results system. The recount confirmed the election results. In 2006, there were recounts in two ward councillor positions. The recounts were held in the same manner as in 2014 whereby the ballots were fed through the tabulators. There was no judge ordered manual paper ballot recount.

Unlike the markings on a paper ballot, voter intent is clear in electronic voting; there is no discretion in interpretation as to how an elector voted. When using paper there can be a great deal of human error since an elector can mark the ballot outside the range of the designated area. The only and most prudent way of recounting internet votes is to re-load the results of the ballots cast.

Internet Voting Statistics

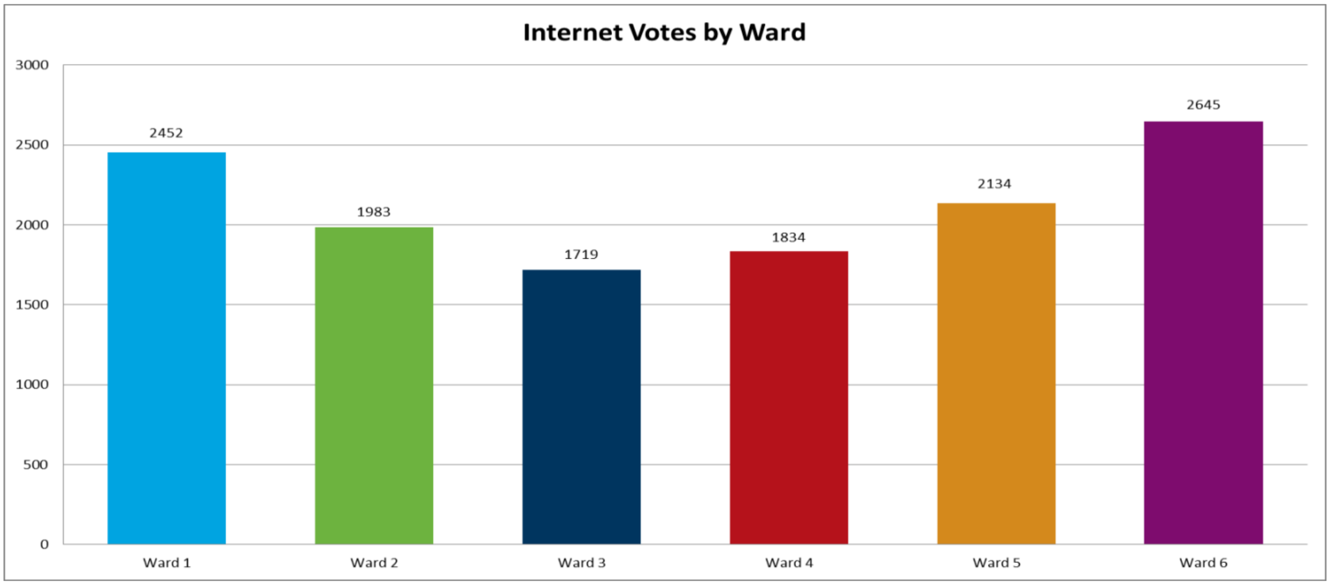
Internet voting has been utilized as an election method in Ontario municipalities since 2003. Since then, adoption has increased and is reflected in the numbers below:

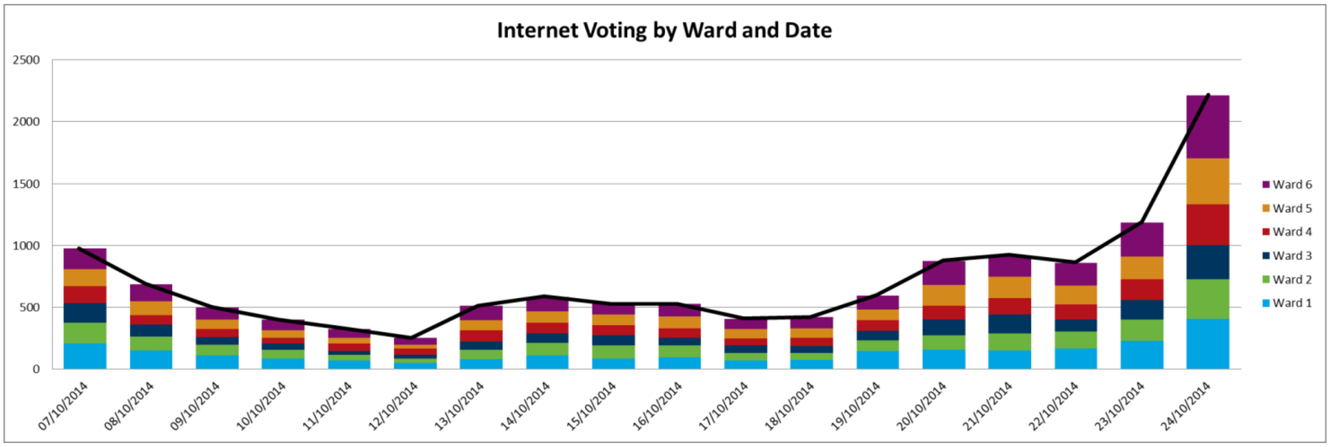
Year	Number of Ontario Municipalities (of 444)
2003	12
2006	20
2010	44
2014	97

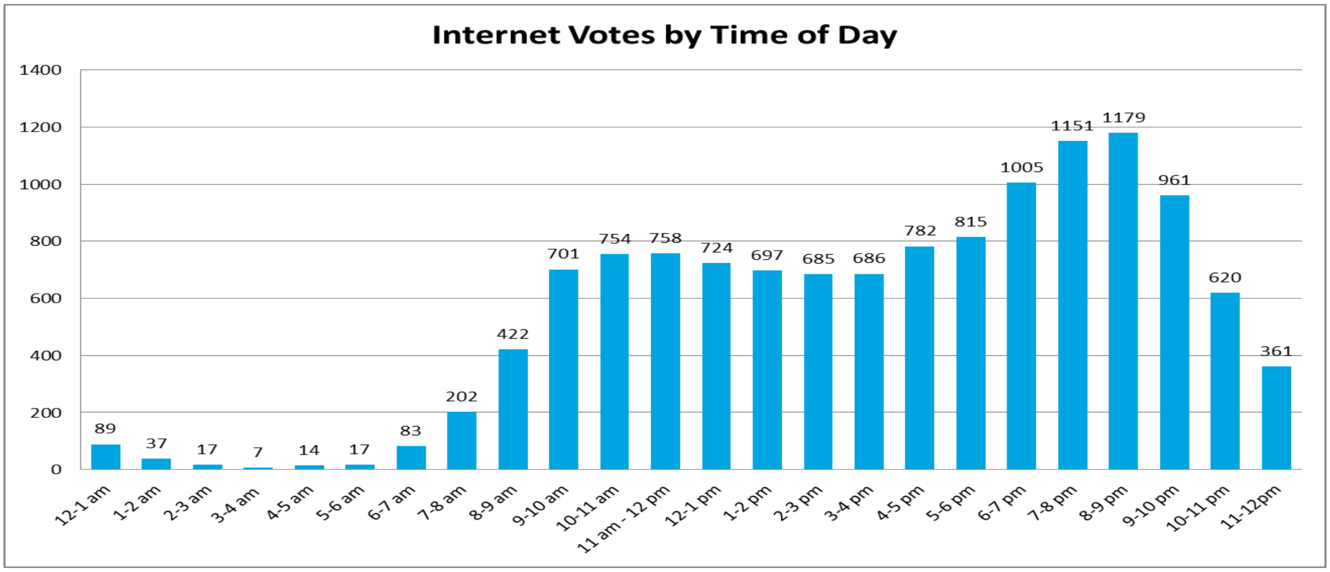
In 2014, 59 municipalities ran fully electronic remote elections. 58 municipalities offered voters a combination of internet voting and telephone voting methods. One municipality offered internet voting only which was the Municipality of Leamington.

As noted in the chart above and in 2014, the City of Guelph was one of the 97 Ontario municipalities that utilized internet voting as a voting method. Internet voting was offered during the advanced voting period only from October 7 to October 24, 2014.

With 432 hours of Internet voting, 12,767 votes were cast online. The following charts reflect the volume of votes over that period of time, breakdown of volume by ward, volume by date and ward and finally time of day when votes were cast.


Internet Votes by Ward
3000
2500
2000
1500
1000
500
0
2452
1983
1719
1834
2134
2645
Ward 1
Ward 2
Ward 3
Ward 4
Ward 5
Ward 6


Internet Voting by Ward and Date
2500
2000
1500
1000
500
0
07/10/2014
08/10/2014
09/10/2014
10/10/2014
11/10/2014
12/10/2014
13/10/2014
14/10/2014
15/10/2014
16/10/2014
17/10/2014
18/10/2014
19/10/2014
20/10/2014
21/10/2014
22/10/2014
23/10/2014
24/10/2014
Ward 6
Ward 5
Ward 4
Ward 3
Ward 2
Ward 1


Internet Votes by Time of Day
1400
1200
1000
800
600
400
200
0
89
37
17
7
14
17
83
202
422
701
754
758
724
697
685
686
782
815
1005
1151
1179
961
620
361
12-1 am
1-2 am
2-3 am
3-4 am
4-5 am
5-6 am
6-7 am
7-8 am
8-9 am
9-10 am
10-11 am
11 am - 12 pm
12-1 pm
1-2 pm
2-3 pm
3-4 pm
4-5 pm
5-6 pm
6-7 pm
7-8 pm
8-9 pm
9-10 pm
10-11 pm
11-12pm

Number of Internet Votes by Age group	
18-24 years old	783
25-34 years old	1,672
35-44 years old	2,427
45-54 years old	2,914
55-64 years old	2,731
65+ years old	2,240
Total	12,767

Summary
In deciding how best to administer the election, Municipal Clerks adhere to the following principles in making determinations under the Municipal Elections Act:

- the secrecy and confidentiality of the voting process is paramount;
- the election shall be fair and non-biased;
- the integrity of the process shall be maintained throughout the election;
- there is to be certainty that the results of the election reflect the votes cast;
- voters and candidates shall be treated fairly and consistently; and
- the proper majority vote governs by ensuring that valid votes be counted and invalid votes be rejected so far as reasonably possible

Further to the above, it is the City Clerk’s responsibility as Chief Returning Officer to ensure that all members of the electorate are given every opportunity to vote and that the voting process is as accessible and accountable as possible.

The intent of the methods of voting recommended, and internet voting in particular, is to assist voters and improve the delivery of election services in relation:

1. improved convenience;
2. enhanced accessibility;
3. opportunity for increased voter turnout.

Risks are prevalent in any voting methodology or system. The City Clerk’s Office understands this and is required mitigate these risks as much as possible. The processes and security measures that have been developed to support internet voting have created a safe and reliable alternative method for electors.

The City Clerk’s Office is confident that all measures possible are being taken to ensure the integrity of the electoral process. The aforementioned information details many of the actions and precautions taken in that regard.

Stephen O’Brien
City Clerk and Returning Officer

City Clerk’s Office
Location: Guelph City Hall, 1 Carden Street, Guelph ON
T 519-822-1260 x 5644
E Stephen.OBrien@guelph.ca

Public Participation in Policy Development

The Key to Efficiency in Evidence-based Policy Development Is Community Engagement

A Presentation To Guelph City Council
April 24 2017

By Hugh Whiteley
hwhitele@uoguelph.ca

Voting Practices in Elections

- The policies that decide who votes and how one votes in elections are of fundamental importance as they have great influence on the integrity of the election results.
- Policies governing voting procedures that are fundamental to the functioning of elected governments must be regularly and carefully reviewed.
- The review of voting procedures should be a fully transparent process using the Guidelines for Community Engagement with early and continuing opportunities for community members to understand what is being reviewed and to contribute to the evaluation of policy alternatives.

Guelph as the epicentre of election fraud

- The criminal conspiracy to manipulate voting that occurred across Canada during the last federal election with its epicentre in Guelph has resulted in greatly increased sensitivity in Guelph electors to the possibility of voting fraud being tried in this City.
- Internet security breaches are sufficiently frequent and serious to require extreme caution in evaluating the security of internet voting systems.

Questions for Council

- Has there been meaningful Community Engagement in the preparation of policy changes in voting procedures ?
- Has there been an in-depth evaluation by experts in system integrity of the security measures needed to ensure the integrity of the election result and prevent fraudulent manipulation of the voting ?

Correspondence Received Regarding:
2018 Municipal Election - Methods of Voting

Dear Mayor Guthrie and Members of Council:

I would like to provide you with access to two key documents which will help inform your decision-making process on Monday.

The first is a 2014 review of City of Toronto internet voting vendor proposals which was prepared by cybersecurity experts.

It was released under a freedom of information access request. It contains very detailed technical analysis of proposals by *Dominion Voting* (the company retained by Guelph in 2014), *Scytl* and *Everyone Counts*.

https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf

This is the key recommendation of the report:

Recommendation regarding the use of internet voting:

Of the proposals evaluated in the context of the RFP process, it is our opinion that no proposal provides adequate protection against the risks inherent in internet voting. It is our recommendation, therefore, that the City not proceed with internet voting in the upcoming municipal election.

A 2016 City of Waterloo staff report on internet voting highlighted a number of key issues which were not covered in the City of Guelph report:

1) The results of an extensive study conducted by Elections British Columbia, and presented to the Legislative Assembly of British Columbia in February 2014, dispel the myth that internet voting increases voter participation in general and participation by young people in particular

2) Internet voting has been successful in a number of jurisdictions but several European countries have decommissioned electronic voting methods due to transparency and security concerns.
And most importantly:

3) Internet voting systems are not 100% hacker-proof despite what vendors may claim when there is proof that so many vastly larger companies and agencies with enormous security expertise and budgets have been successfully penetrated.
You can access the original report via this link:

http://www.waterloo.ca/en/calendar/council/Default.aspx?StartDate=11/21/2016&EndDate=11/21/2016&Limit=25

Click on "original packet" and go to page 99.

Sincerely,
Susan Watson

Chris Cates
111 Royal Terrace
Edmonton, AB   T6J 4R2

March 15, 2017

Elected representative,

I would like to thank you for taking a moment to read this letter as I know your time is valuable. My name is Chris Cates and I am a Canadian citizen residing in Edmonton, Alberta. I am an entrepreneur, a computer programmer, and have been working in the IT sector for over 20 years. I tell you this so you understand I am not a technophobe or a luddite.

I am writing you today because I have learned you are considering an option to make use of internet voting technologies for future elections. Most likely, you are being told online voting will save money, increase voter turnout, speed up tabulation and can be conducted safely & securely. As I will explain, and provide evidence to support, you will see how there is very little, if any, truth in these claims.

Increased Turnout
One of the biggest reasons governments are considering internet voting is the hope the technology will somehow miraculously cure voter apathy. You may have heard the claim turnout rose 300% because of online voting. This was Markham, ON during their 2003 municipal election. While true, there was an increase in turnout, this was only for the advanced voting period; actual turnout for the entire election was a dismal 26.71%.[1] Sadly, biased manipulative statistics like this are used often by sales reps and other advocates with vested interests in internet voting, but when statistics for overall elections are examined we see only marginal increases, if any.

> ***"Other presumed benefits, such as increased turnout and lower cost are not typically realized."***
> *Independent Panel on Internet Voting Recommendations Report to the Legislative Assembly of British Columbia*[2]

It's not uncommon to see drops in turnout where online voting used either. In Markham, only 17.09% of voters cast ballots online in 2003. In 2010, after heavy advertising, 16.07% voted online. Even the Halifax Regional Municipality (HRM), who used online voting in their 2016 election, and saw a drop of over 10,000 e-voters when compared to 2012.[3] Similar statistics can be seen in other locations around the world where internet voting is used, including Estonia.

Another claim made by proponents, is it will increase turnout with younger voters because they supposedly live their lives online. However, statistics prove there is no additional increase in turnout for younger voters either. In fact, according to director of the Center For E-Democracy, Nicole Goodman, the average age of the internet voter is 53 years old and already votes in past elections with a mere 4% of all internet voters being 18-24 years of age.[4]

[1] R. Gosse, Director of Legislated Service/City Clerk, November 2, 2012 – Staff Report "Alternative Voting – Internet Voting" (http://katemdaley.ca/wp-content/uploads/2013/01/FCS-12-191-2.pdf)

[2] Independent Panel on Internet Voting, February 2014, Recommendations Report to the Legislative Assembly of British Columbia (http://www.internetvotingpanel.ca/docs/recommendations-report.pdf)

[3] Metro News, October 13, 2016 – Halifax Votes 2016: E-voting Turnout Down By More Than 10,000 From 2012 (http://www.metronews.ca/news/halifax/2016/10/13/halifax-votes-2016-e-voting-turnout-down-from-2012.html)

[4] Nicole Goodman & Leah C. Stokes, October 6, 2016 – Reducing the Cost of Voting: An Empirical Evaluation of Internet Voting's Effect on Local Elections (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849167)

> ***"Our estimates suggest that internet voting is unlikely to solve the low turnout crisis"***
> Nicole Goodman & Leah C. Stokes, Reducing the Cost of Voting: An Empirical Evaluation of Internet Voting's Effect on Local Elections

Goodman's statistics show on average a mere 3% increase in turnout may be realized. If online voting truly increases turnout, why aren't we seeing large increases where it's used? If online voting enables younger voters to vote, why are they not voting? Perhaps more research is needed to understand voter apathy and how it can be solved rather than wasting resources on unproven technology in blind hope of affecting turnout.

We Can Bank Online, Why Can't We Vote Online?

Perhaps you've even thought this yourself at one point. The answer is quite simple; voting is anonymous, banking is not. Paying taxes, shopping, or banking online all link you and your information to each transaction allowing everything to be audited and irregularities detected.

Despite all of this, online banking isn't very secure. Numerous viruses like Zeus[5], Citadel[6], and SpyEye[7], were specifically written to infect a computer and steal banking information. Even secure online financial systems, like SWIFT, have lost millions of dollars because of hackers.[8] If banks can't keep hackers from stealing from their secure online systems, should we really believe anyone who says they can keep online votes secure?

Voting, on the other hand, is required by law to ensure all ballots are kept secret. Article 163 of the Canada Elections Act (S.C. 2000, c.9) states; "The vote is secret". Nothing must link vote to voter, but computers are designed to prevent unauthorized anonymous access, which makes it impossible for a "secure" computer to record a digital ballot without linking some information back to the voter. To maintain the principle, One person, One vote, a computer system must record who voted, and to ensure any kind of accuracy the computer system must link vote to voter. This is especially true for online voting systems which allow a voter to change their vote before the end of the election.

Proof in point, the canceled primary in 2016 for the Russian Party of People's Freedom (PARNAS) party. Hackers broke into the secure online voting system and published voter names, phone numbers, e-mail addresses, login credentials, and even the candidate they voted for.[9] Also, when the non-profit organization, Electronic Frontier Finland (Effi), audited an e-voting system created by Scytl for the Finish government in 2008 their report stated:

> ***"It is possible to find out how an individual voter voted, as votes are processed in an unencrypted form during the counting process, with voter-identifying information attached to each vote. It seems that ballot secrecy could be compromised by system programmers or a group of insiders having access to all decryption keys"***[10]

[5] Wikipedia, No Date – Zues (Trojan Horse) (http://en.wikipedia.org/wiki/Zeus_(Trojan_horse))

[6] ThreatPost, February 1, 2013 – Citadel Trojan: It's Not Just For Banking Fraud Anymore (http://threatpost.com/citadel-trojan-it-s-not-just-banking-fraud-anymore-020113/77481)

[7] Daily Mail UK, January 6, 2012 – New PC Virus Doesn't Just Steal Your Money – It Creates Fake Online Bank Statements So You Even Don't Know It's Gone (http://www.dailymail.co.uk/sciencetech/article-2083271/SpyEye-trojan-horse-New-PC-virus-steals-money-creates-fake-online-bank-statements.html)

[8] New York Times, May 12, 2016, - Once Again, Theives Enter Swift Financial Network and Steal (http://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html?_r=0)

[9] RT – Opposition PARNAS Party Cancels Primaries Over Massive Leak of Voters' Personal Data (https://www.rt.com/politics/344827-voters-personal-data-leaked-online/)

[10] Electronic Frontier Finland (Effi), November 28, 2009 – A Report on the Finnish E-Voting Pilot (http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf)

Costs Less

Some argue internet voting costs less than paper based elections. This can only be true when internet voting is the only method of voting with no polling stations, and even then, are all costs related to the election being considered? There are numerous costs associated with online voting often not taken into account, such as: advertising, promotional/informational mailings, postage, translation, voter technical support, or IT overhead for additional staffing, database administration, network security, security audits, IT technical support, etc.

Most municipalities using online voting offer the technology as an alternative method of voting in addition to paper ballots. Thus, the election costs typically rise because yet another means of voting is being added which requires administrative overhead. Municipalities can see election costs double, even triple, by adding an internet voting option when they are being told it will save money. As detailed in their respective staff reports, Kitchener[11] & Waterloo[12] projected enormous additional costs related to the use of internet voting and these municipalities are just a couple Ontario of examples.

No matter how much technology we have, nor how much cost savings that technology can provide, there are some things in our world which we all must do in person. Like taking the road test for our driver's license, or showing up to work everyday. We have the technology right now to allow everyone to take a virtual road tests or work in virtual offices. Still, millions of people everyday make their way to brick and mortar buildings to do the things which must be done in person. Take road tests. Work. Even do their shopping and banking. There are numerous reasons why people should show up to cast their ballot in person, but the most important is to ensure an actual person is casting an actual ballot.

Upholding Democratic Principles

Before you consider using any form of electronic voting (internet, telephone, electronic tabulation, etc.), we should first take into consideration the key principles of a democratic election. If these principles cannot be upheld, then it is our responsibility to reject the technology to protect our not only elections but also our democracy.

These core principles are:

- Ensure only eligible electors can vote
- Eligible electors can only cast one ballot
- Each elector's identity must not be linked to their ballot
- Election results can be audited and independently verified
- Security of the voting system is ensured

With online voting, can we ensure only eligible electors can vote and cast only one ballot? No. The simple fact is there is no way to prevent a voter from casting multiple ballots. So long as the person has the right credentials they can cast a ballot whether they are eligible or not. It is simply too easy for someone to collect the right information to cast ballots for friends or family.

There have already been numerous elections in Canada where people have voted multiple times using online voting to do so. The RCMP is investigating at least one case of voter fraud where a voter's information was used to cast a ballot by another person during the 2016 electoral reform plebiscite conducted using Simply Voting's online voting platform in P.E.I.[13] In October 2010, Peter Byvelds, was able to cast five ballots by stealing PIN codes of family members and casting

[11] City of Kitchener, November 2, 2012 – Staff Report, Alternative Voting – Internet Voting (http://katemdaley.ca/wp-content/uploads/2013/01/FCS-12-191-2.pdf)

[12] City of Waterloo, November 21, 2016 – Staff Report, Alternative Voting Methods (Internet Voting) (https://www.doesyourvotecount.ca/wp-content/uploads/2016/11/City-of-Waterloo-CORP2016-105.pdf)

[13] CBC News, November 8, 2016 – Elections P.E.I. Not Ready To Recommend Online Voting In Next Election (http://www.cbc.ca/beta/news/canada/prince-edward-island/pei-plebiscite-online-voting-1.3841893)

their ballots in addition to his own.[14] In 2014, Alberta PC party members received two PINs allowing them to successfully vote twice, while others couldn't vote at all during the leadership election conducted using Scytl's online voting system. Also in 2014, a City of Sudbury employee was able to cast two ballots, one online and one on paper, without being detected by the online voting system provided by Scytl.[15]

During this election, David Duffy was able to register the web address: *greatersudburyvotes.com* (the real website for the election was: *greatersudburyvotes.ca*) and successfully set up a fake voting website which looked identical to the real voting website.[16] This type of man-in-the-middle cyber-attack is just one way for one person to greatly affect the outcome of an entire election. And this is just one of thousands of tactics which can easily be employed to capture the necessary information so ballots can be altered without detection by the voter, election officials, and/or the online voting platform.

Often people think a simple audit of the votes cast will ensure accuracy and inspire trust with the online votes, but how do you audit a digital ballot? Unlike paper ballots which can be recounted and independently verified, there is no way to recount digital ballots. There is no way to ensure the digital ballot was not altered on the client computer or the online voting system. In fact, there is no way to prove whether an actual person even cast the ballot. Bots are used continually employed to make their way through 'secure' ticket purchasing platforms so they can buy up tickets to concerts and other events.

Can election results be audited and independently verified? No. Ernest & Young was contracted to 'audit' the Halifax Regional Municipality (HRM) election which used Scytl's online voting system. Their report stated quite clearly:

> ***"The Specified Auditing Procedures performed do not constitute an audit or review engagement and, accordingly, no assurance is expressed."***[17]

How can the public be confident in any election where ballots cannot be independently audited to verify results and ensure accuracy? By approving online voting, you're asking citizens to blindly trust election results provided by a private, third-party, for-profit, contractor who has no obligation to prove results are accurate nor report if they get hacked. Why would any government allow this? Why would anyone expect the public to accept this?

Security of the voting system cannot be ensured

When thinking about security remember "secure" is relative term. Is your home secure when you close all the windows and lock the doors? To a degree, it is, but if a burglar wants to break-in they can. Is your home secure when you install a large fence, a guard dog, a security system and cameras? Again, to a degree, it is, but once again a determined burglar can still get in.

This understanding of security can be applied to computer security as well. There are levels of security which can be applied to make a computer or a network more secure, but in all instances this security can still be breached. Take, for example, the ultra-secure U.S. Pentagon computer system which was hacked in 2011.[18] This was no simple website

[14] Standard-Freeholder, April 19, 2011 – Man Fined $1,500 For Casting Five Votes (http://www.standard-freeholder.com/2011/04/19/man-fined-1500-for-casting-five-votes)

[15] CBC News, October 22, 2014 – Greater Sudbury worker votes twice in election (http://www.cbc.ca/news/canada/sudbury/greater-sudbury-worker-votes-twice-in-election-1.2809664)

[16] CBC News, October 23, 1014 – Creator of Greater Sudbury fake voting web site 'shocked' by oversight (http://www.cbc.ca/news/canada/sudbury/creator-of-greater-sudbury-fake-voting-website-shocked-by-oversight-1.2810069)

[17] Ernest & Young, October 23, 2012, Specified Auditing Procedures Report Electronic Voting (http://www.halifax.ca/election/documents/HRMSpecifiedProcedures-E-Voting2012-FinalReport.pdf)

[18] Huffington Post, September 13, 2011 – Foreign Hackers Stole 24,000 Military Files, Pentagon Says (http://www.huffingtonpost.com/2011/07/14/foreign-hackers-stole-240_n_899304.html)

defacement. Over 24,000 files detailing surveillance technologies, satellite communications, and network security protocols were just some just some of the documents stolen from their network during the breach. Even the Canada Revenue Agency (CRA) had to shut down its web site when it fell victim to the Heartbleed[19] vulnerability in April of 2014.[20]

Giant technology companies like Microsoft, Apple, Cisco, Adobe, and Google, to name a few, release software patches and security updates numerous times each year to patch vulnerabilities. These companies are innovators of technology earning billions in revenue, yet with all the advancements in various technologies, vulnerabilities with their software still exist and new exploits are found all the time. If companies and financial institutions haven't cornered the market on computer security, why should we believe the exaggerated security claims made by online voting companies or their proponents?

If voting companies had some special technology to make their systems more secure and unhackable, why wouldn't they be marketing it to governments, banks, or other corporations who would pay handsomely for it? The simple fact is, they are just as vulnerable to security problems as every other technology company today. Perhaps this is the reason why these companies do not allow public tests of their voting systems. When you are being told, online voting is secure, please consider who is making the claim. Does this person have the knowledge and expertise in computer security to be able to make such a claim? Or are they simply repeating claims made by online voting vendor and their advocates? Do they represent an online voting company which has a vested interest in your decision? For you to make an informed decision, it is imperative to know where these often over-emphasized and exaggerated security claims are coming from.

Computer scientists, professors, and other technology experts around the world are speaking out against the use of online voting because they know the internet is no place to hold an election. These scientists are exposing security vulnerabilities in online voting systems used in Estonia[21], Australia[22], and going so far as to openly hack platforms like the proposed Washington D.C.[23] online voting system. Western University assistant professor, Aleksander Essex, successfully hacked the open-source, open-audit, cryptographic end-to-end (E2E) internet voting system of Helios and found it was possible for an election official to rig the results, or have a voter send a poisoned ballot to stop vote tabulation, or a vote stealing attack could occur where an attacker could cast ballots on a voter's behalf.[24] What vulnerabilities exist in the 'secure' internet voting systems we are prevented from examining?

The use of phishing scams, ransomware, trojans, and other malware is increasing and IT professionals are admitting they can't keep up. In the 2017 report from FireEye[25], it has been determined that cyber criminals now possess the abilities to operate on the same levels as nation states. They also noted it takes on average 99 days for security breaches to be identified. This means online voting systems could be opened and closed and never know a breach has occurred. These trends are worrisome, and just as alarming is a recent survey conducted by Mozilla[26]. It found 90% of internet users don't

[19] TechCrunch, April 7, 2014 – Massive Security Bug In OpenSSL Could Affect A Huge Chunk Of The Internet (http://techcrunch.com/2014/04/07/massive-security-bug-in-openssl-could-effect-a-huge-chunk-of-the-internet/)

[20] CBC News, April 9, 2014 – Heartbleed Bug May Shutdown Revenue Canada Website Until Weekend (http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742)

[21] J. Alex Halderman, November 2014 – Security Analysis of the Estonian Internet Voting system (https://jhalderm.com/pub/papers/ivoting-ccs14.pdf)

[22] Vanessa Teague, April 2015 – The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election (https://arxiv.org/pdf/1504.05646v2.pdf)

[23] J. Alex Halderman, June 2012 – Attacking the Washington, D.C. Internet Voting System (https://jhalderm.com/pub/papers/dcvoting-fc12.pdf)

[24] Aleksander Essex, December 2016 – The Cloudier Side of Cryptographic End-to-End Verifiable Voting: A Security Analysis of Helios (https://whisperlab.org/helios/helios.pdf)

[25] FireEye, March 2017, M-Trends 2017 (https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html)

[26] Mozilla, March 2017 – Hackers, Trackers and Snoops: Our Privacy Survey Results (https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5#.a5c2a0apb)

know how to protect themselves online. Over 30,000 participants from around the world (Canada, USA, UK, France, Germany, etc.) admitted they know “little, but not enough” about securing their internet connected devices, and feel they “have no control at all” over their personal data. How can any election conducted online be secure if the people casting the votes do not know enough about securing their systems? How easy will it be for a hacker to manipulate their computer or smartphone to alter their vote?

You don’t have to take my word for it.

> ***“The security risks associated with Internet voting pose a serious threat to a number of these principles. The Clerk is committed to exploring technological and other solutions that improve voting accessibility but remains of the opinion that current Internet voting systems are not secure enough for large scale use in binding, public elections.”***[27]
> City Clerk, Toronto, Ontario, Executive Committee Report for Action

> ***“Do not implement universal Internet voting for either local government or provincial government elections at this time.”***
> ***“The risks of implementing Internet voting in British Columbia outweigh the benefits at this time.”***[28]
> *Independent Panel on Internet Voting Recommendations Report to the Legislative Assembly of British Columbia*

> ***"I still think the in-person voting is the most secure and safe way of voting."*** [29]
> Gary McLeod, P.E.I. Chief Electoral Officer

> ***“Should we start using Helios for public-office elections? Maybe US President 2016?***
> ***No, you should not. Online elections are appropriate when one does not expect a large attempt at defrauding or coercing voters. For some elections, notably US Federal and State elections, the stakes are too high, and we recommend against capturing votes over the Internet. This has nothing to do with Helios itself: we just don’t trust that people’s home computers are secure enough to withstand significant attacks.”*** *[30]*
> *Internet Voting Maker, Helios Voting*

> ***“Internet voting may well remain a good idea for private elections, for EBAs, and for popular events but it will never have the qualities needed for high stakes public elections even party elections with outcomes affecting the general public.”***[31]
> Craig Burton, founder of online voting maker, Everyone Counts

[27] Toronto, ON City Clerk, November 17, 2016 – Changes to the Municipal Election Act and Related Matters Impacting the 2018 Election (http://www.toronto.ca/legdocs/mmis/2016/ex/bgrd/backgroundfile-98545.pdf)

[28] Independent Panel on Internet Voting, February 2014, Recommendations Report to the Legislative Assembly of British Columbia (http://www.internetvotingpanel.ca/docs/recommendations-report.pdf)

[29] CBC, October 27, 2016 – Everyone’s Watching The P.E.I. Plebiscite (http://www.cbc.ca/news/canada/prince-edward-island/pei-plebiscite-electoral-reform-electronic-voting-observers-1.3811752)

[30] Helios Voting, date unknown – Helios Voting FAQ (https://vote.heliosvoting.org/faq)

[31] Craig Burton, November 4, 2016 – Inquiry Into and Report on All Aspects of the Conduct of the 2016 Federal Election and Matters Related Thereto (http://www.aph.gov.au/DocumentStore.ashx?id=cef80a64-c984-4628-9de7-41640c25a978&amp;subId=459751)

> ***"Despite the fact that Simply Voting is a major Canadian internet voting vendor, its recommendation is against the use of internet voting for federal elections. The heightened threat level of a federal election pushes the security of internet voting past its limits and poses too much of a risk."***[32]
> Brian Lack, founder of online voting maker, Simply Voting

After learning over 68.8% of the Canadian public are either concerned or very concerned about reliability and security of online voting, and hearing about the risks from one computer security expert, the Special Committee on Electoral Reform for the Canadian House of Commons in 2016 stated quite clearly in their report:

> ***"The Committee recommends that online voting <u>not</u> be implemented at this time."***[33]
> Francis Scarpaleggia, Chair of the Special Committee on Electoral Reform

Conclusion

This statement echoes numerous reports and finding by other organizations across Canada and elsewhere around the world which state that it is simply too risky to put our elections online. As you can see from the evidence I have provided, it is highly unlikely online voting will save money or increase turnout. There is no means for online voting to be properly audited to prove election results, prevent voter coercion, or stop one person from casting numerous ballots. Current technology cannot be made secure enough to ensure no person, hacker, or malware affected the outcome, nor does it allow recounts to ensure accuracy.

Please respect the democracy our forefathers fought and died to protect.
Please protect the democratic principles and ensure our elections can continue to be transparent, verifiable, and trustworthy.
Please reject the use of online voting!

> ***"Those who cast the votes decide nothing. Those who count the votes decide everything!"***
> *Josef Stalin*

Respectfully,

Chris Cates

[32] Simply Voting, September 20, 2016 – Simply Voting Submission to the Special Committee on Electoral Reform (http://www.parl.gc.ca/Content/HOC/Committee/421/ERRE/Brief/BR8463279/br-external/SimplyVoting-e.pdf)

[33] Special Committee on Electoral Reform, December 2016 – Strengthening Democracy in Canada: Principles, Process and Public Engagement For Electoral Reform (http://www.parl.gc.ca/Content/HOC/Committee/421/ERRE/Reports/RP8655791/421_ERRE_Rpt03_PDF/421_ERRE_Rpt03-e.pdf)

To City Council;

Make easy to use online voting for computers and Mobile. It will actually lead to better functioning cities, especially when combined with effective leaders and citizens who care about tomorrow.

All others signals have led to ever lower levels of citizens voting making government invisible and irresponsible decisions. It leads to better engagement and a chance to create a regular mobile app for those who are set to rule and share power.

Get it right, Guelph and be an example and pioneer for fearless leadership and forward thinking cities.

Sincerely,

Paul Z Peteranac

***

Dear Councilor,

I strongly ask you to either stay steadfast in your stance against online voting, or to seriously consider changing your stance if it is pro-online voting.

Waterloo councilors voted unanimously against online voting. Please ask them why an entire council would do this? Is it because Waterloo is a technologically regressive City? Waterloo University in itself is ranked among the top universities in the world for Computer Science, so the reason may be quite the opposite.

Across the board computer scientists, network creators, and software engineers will tell you that the internet is not nearly safe enough for something as sensitive as voting. You will know this already if you have done your homework.

**When we have a situation where someone can vote online, masquerading as their child who is away at university, is a situation that we *should not* have online voting.

**When we have political parties and politicians who abuse the internet by stealing their opponent's websites or foster robocalls that confuse voters about polling stations, is a situation that begs we *should not* have online voting.

Please take my request seriously and investigate the issue, leaving convenience behind as a viable pro to online voting. Convenience has lead us down many roads that make life easier in the short run, but far harder in the long run.

Sincerely,

-T. Shawn Johnson

***

April 12, 2017

Mayor and Council,

City of Guelph

Subject: Internet Voting in 2018

Dear Mayor and Council,

I am opposed to the use of internet voting in the 2018 municipal election – for both the advanced poll and on election day. I will outline my thoughts below, and then list some links to supporting documents.

1. **We cannot guarantee that a computer system is secure.** I have worked in the computer / IT industry for 30 years, and I have come to the conclusion that we cannot guarantee the security of any computer system. We regularly hear new reports about hackers compromising systems, from personal computers to large corporate servers. I expect that most of you know someone who has had their computer infected by a virus or ransomware, or had their email contact list used to send fake messages. Hackers can be hired to break into specific systems, and their job is made easier by using available hacking toolkits. I will question the judgement of anyone who claims that a particular system is 100% secure.
2. **Elections are different than online banking and shopping.** Banks and online retailers accept that there is some risk to online transactions, and they will compensate customers for a loss due to unauthorized transactions. In an election however, one vote can decide a race, and there is no way to compensate the losing candidate and their supporting voters. I don't think any of us agree that it is ok for 2 or 3 percent of votes to be fraudulent. Banks and retailers accept a 2 or 3 percent loss as a cost of doing business. It should not be a part of the election business.
3. **There was no problem last time / other municipalities do it.** We don't actually know that there were no problems last time. If a hacker is doing their job well, there may be no trace of the hack. In any case, if we and other municipalities have not had problems in the past, it does not mean the future is secure. It is like leaving one's car unlocked with the key in it – you might go for years with no problem, but sooner or later it will get stolen.
4. **We must have absolute faith in our Election process.** In a democratic society, we count on elections to reflect the will of the people. If there is doubt in the security of the election process, then we cannot be sure of the result, and the whole process breaks down.

In conclusion, I ask you to reject internet voting for the entire 2018 election. The internet voting system cannot be guaranteed to be secure, and our election process must be a trustworthy as we can make it.

Sincerely,

Geof Kearns

***

Please pass these thoughts along to council concerning online voting.

Mayor Guthrie has asked the citizens of Guelph to write to their council members in support of on line voting. I am afraid that I have serious concerns about rushing into accepting online voting until we can be reasonably assured that the system cannot be easily manipulated. I realize that no system can be made 100% foolproof. When you hear about government agencies like the CIA and the NSA let alone numerous large corporations having their computers hacked despite the resources they would have to prevent such an occurrence I wonder if the city has the resources to provide a system that the citizens can be confident of. There must be procedures in place to check that systems are working as they should including the ability to check that the software running the system is doing what we think it is doing. An extreme example could be a system where say every tenth vote for candidate A gets transferred to candidate B. Without the ability to check what the software is doing how would we know. Before you dismiss this as being far fetched the Robocall fiasco a few years back shows how far some parties will go and how much effort they will invest in order to swing an election in their favour. As you all know it happened right here in Guelph. If I am voting online from home how do I know that I am not being sent to a website that looks like the real one, but in reality is a bogus one where all my information is recorded and then used to cast a vote for a different candidate. The police are constantly warning people about similar sorts of scams, bogus Canada Revenue Agency websites come easily to mind. Many other concerns such as out of date voters lists and the possibility that a domineering family member may force other members to vote for a certain candidate have also been raised and need to be addressed. I realize that online voting is a convenience for some people and it may encourage more people to vote which is a definite positive, however I believe if they are made aware of how easily the system could be abused they may have second thoughts. We need to make sure that sufficient checks and balances are in place to guard against such abuse before we rush into online voting.

Thank you.
Glen Wilson

***

Dear Mayor Guthrie, City Clerk and Councilors,

I feel internet voting should be rejected until voters lists are accurate and security is reliable.

I have no knowledge of security issues in elections (other than the being a victim of the robocall mis-direction). From what I read, however, internet security is a major concern.

But I have used the voters list while helping to plan a municipal-level campaign a few years ago. It was by far our biggest headache, riddled with mistakes and extremely out-of-date. Unless it has been completely overhauled since then and kept up-to-date, or a better list has been found, I cannot see how it it could be the basis for a valid internet vote. I feel its use would make a mockery of municipal democracy, with costly consequences in both unreliable results and the expense of dealing with the mess.

Elizabeth Snell

***

To the Mayor and Councillors:

Because there is the potential of hackers I am opposed to online voting.

Sandy Nicholls

***

Dear City of Guelph Council members:

I am concerned that the Mayor's ill-advised push to institute online voting will, if successful, expose the city's citizens not only to possible erroneous election results and lost votes, but also to potential election fraud.

I support Council in the decision to defer online voting to a time in the future when security can be more certain. Councillors are obligated to protect the integrity of the vote, and the technical advisors who study internet security have evaluated that now and in the near-term future, online elections can not yet be made secure.

Voting convenience for the needs of particular populations can be provided as it has been in the past, and no citizen's vote need go uncast or uncounted. Please oppose Mayor Guthrie's attempt to disregard risk and hurry the adoption of online voting, and keep us out of potentially risky internet use.

Sincerely,

Sally Ludwig

***

I'm a devotee of the Internet. I am also strongly against e-voting until it's proven secure. There is no proof.

This article tells the story: https://goo.gl/g730xJ

"Proposals to conduct voting pilots using real elections continue to reappear both in the U.S. and elsewhere, **seemingly independent of warnings from computer security experts**. While the appeal of Internet voting is obvious, the risks, unfortunately, are not, at least to many decision makers. Yet voted ballots sent via Internet simply cannot be made secure and make easy and inviting targets for attackers ranging from lone hackers to foreign governments seeking to undermine US elections."

Those conclusions cannot be dismissed. They are alarming.

What concerns me more is the dramatic push for e-voting by the mayor and a few other council members.

Convenience is good, sure. Helping the disabled is good, of course.

But Internet fraud that could be used by cheaters to skew the vote — or the intense bombardment of manipulative marketing messages imploring voters to push a button — are risks that make convenience and the rights a relative few people seem like a weak pretense.

Why the imprudent urgency? Why all the tweets?

If a political organization is adept at using the Internet to communicate, promote, and god-forbid manipulate, it has a distinct advantage if voting is done by Internet.

No such advantage should exist.

Our traditional voting confers no such advantage. E-cheating can't happen.

Our traditional voting method is a level playing field. Internet voting might not be.

The question for councillors: If the implications are all considered — including insecurity and fraud — what are you voting for?

As the mayor wrote in big, bold typography on his website, "What you allow is what will continue."

Precisely the point.

Tony Leighton

P.S. "An avalanche of emails" coming to city hall that are lopsidedly pro any one issue can be triggered by an Internet-savvy political organization with a big mailing list and an alarmist marketing message, and is, in fact, a perfect demonstration of how the Internet can skew democracy. It is not an accurate measure of how Guelph feels.

***

To Mayor & Council,

Like most people, I naively assumed electronic voting was a positive step for democracy. Until I studied the evidence. Since you've been presented with loads of persuasive evidence already, I have to assume that you too have come to understand that the risks aren't worth it. Not even close.

This is not about ideology, so please don't try and paint it that way. This is about maintaining our viability as a democracy, plain and simple. There is just no way that technology is even close to ensuring that Guelph won't be subject to (invisible) fraud and manipulation. Surely you can see that?

I have read the "pro" arguments, and they aren't really arguments because they don't acknowledge the seriousness of fraud. Of course we all want greater voter turn-out in an accessible manner. So let's put our energy into ensuring that the marginalized and the disenfranchised have their vote count next election without having to rely on a computer. It's done all over the world.

Tom Klein Beernink

***

Dear Councillor Salisbury,

Why are you, along with 6 other City Councillors (Bell, Gordon, Allt, Hofland, Piper, Wettstein) in favour of ending online voting without even trying to fix a single problem?

Now I'll admit, I don't recall voting online in 2014, but when 13,000 people (33% of eligible voters) voted online in advance of Election Day; you have to admit two things: 1. That's democracy at it's best, 2. That it's use for the first time was a success.

I was hoping to try online voting in 2018 and now you, along with Councillors Bell, Gordon, Allt, Hofland, Piper, and Wettstein are going to take it away? I'm sorry but ending online voting does not count as fixing it! If there is a problem with Guelph's online voting system, please try to fix it, for democracy's sake!

If the voters list is a problem, is it even possible to get a list of eligible voters from either Elections Ontario or Elections Canada?
Ontario does go to the polls that same year (2018). (Getting the list from MPAC could be the problem, just saying).

Another reason why we have to keep online voting: it's very popular among my generation (18-34 Year Olds). For the record, I'm currently 33, but will be turning 34 in October. Now do you want to get people my age out to the polls? If you do, ending online voting does not work in getting them out.

Now as to why I'm emailing you directly Councillor Salisbury is that you happen to represent my Ward (Ward 4). As to why CC'ing the other 6 who want to end online voting (Councillors Bell, Gordon, Allt, Hofland, Piper, and Wettstein) is that I felt they needed to hear what I had to say.

Before you go into you Council Meeting on April 24, please change your votes and keep online voting either the way it is, or fix any problems that the current system may have. As I said earlier, this is for democracy's sake!

Thank You in advance,

Russ Peebles

***

TO:

Cameron Guthrie, May of Guelph
Members of City Council.

FROM:
Michael Keefer, D.Phil.,
Professor Emeritus, University of Guelph.

Dear Mayor Guthrie and Members of Guelph City Council,

I am writing to you on the subject of Internet Voting. I understand that the April 3, 2017 recommendation of Council's Committee of the Whole, which is to disallow any internet voting in the 2018 civic election, will go to Council for a final decision on April 24.

I urge you and your colleagues to endorse the April 3 recommendation, and to ensure that internet voting--which poses a mortal threat to the integrity of any election based on it--is not incorporated into any future municipal election.

I do not claim expertise in computer programming, IT, or electronic security issues. However, since 2003, a year before I began myself to publish on issues of election integrity and electoral irregularities, I have read widely among the writings of computer security experts like Bruce Schneier, Rebecca Mercuri, and Aviel Rubin who have taken a special interest in electoral applications of their research, and also among the writings of election integrity experts such as Bob Fitrakis, Steve Freeman and Mark Crispin Miller. I have myself published half a dozen scholarly papers and a larger number of journalistic articles on electoral irregularities in the U.S., Haiti, Canada and elsewhere.

This might be an appropriate place to note that I have recently read the message addressed to you on March 17, 2017 by Edmonton entrepreneur and computer programmer Chris Cates--which I would endorse as a very knowledgeable and thoroughly researched exposition both of the false promises held out by internet voting, and also of the very serious impact it could have on the integrity of our elections.

I would like to supplement what Mr. Cates says by referring briefly to a report on the risks of internet voting that has been recommended by Bruce Schneier (who is, by the way, the Chief Technology Officer of IBM Resilient, a Fellow at Harvard's Berkman Center, and a member of the Electronic Frontier Foundation). The report, co-authored by Catriona Fitzgerald of Electronic Privacy Information Center, Pamela Smith of Verified Voting Foundation, and Susannah Goodman of Common Cause Education Fund, is entitled "The Secret Ballot at Risk: Recommendations for Protecting Democracy"; it is available at http://secretballotatrisk.org/. One of the conclusions of this report is that although "the right to cast a secret ballot in a public election is a core value" of democracy, "it is impossible to maintain separation of voters' identities from their votes when Internet voting is used. Most [U.S.] states that offer Internet voting recognize this limitation and require voters to sign a waiver of their right to a secret ballot." The authors also remark that the risks involved in transmitting marked ballots via the internet--in other words, the risks involved in internet voting--"are overwhelming and it should not be an option."

I would like to quote as well from an important document published by another leading computer security expert, "Rebecca Mercuri's Statement on Electronic Voting," available at http://www.notablesoftware.com/RMstatement.html. Dr. Mercuri's comments in this statement include the following:

--"Fully electronic systems do not provide any way that the voter can truly verify that the ballot cast corresponds to that being recorded, transmitted, or tabulated. Any programmer can write code that displays one thing on a screen, records something else, and print yet another result. There is no known way to ensure that this is not happening inside of a voting system."

--"No electronic voting system has been certified to even the lowest level of the U.S. government or international computer security standards (such as the ISO Common Criteria or its predecessor, TCSEC/ITSEC), nor has any ever been required to comply with such."

--"Encryption provides no assurance of privacy or accuracy of ballots cast. Cryptographic systems, even strong ones, can be cracked or hacked, thus leaving the ballot contents along with the identity of the voter open to perusal."

--"Internet voting (whether at polling places or off-site) provides avenues of system attack to the entire planet. If the major software manufacturer in the world cannot protect its own company and products from an Internet attack, one must understand that voting systems (created by this firm or others) will be no better (and probably will be
worse) in terms of vulnerability."

--"Off-site Internet voting creates unresolvable problems with authentication, leading to possible loss of voter privacy, vote-selling, and coercion. Furthermore, this form of voting does not provide equal access for convenient balloting by all citizens, especially the poor, those in rural areas not well served by Internet service providers, the elderly, and certain disabled populations. For these reasons, off-site Internet voting systems should not be used for any government election."

Dr. Mercuri insists that "It is [...] incumbent upon all concerned with elections to REFRAIN from procuring ANY system that does not provide an indisputable, anonymous paper ballot which can be independently verified by the voter prior to casting, used by the election board to demonstrate the veracity of any electronic vote totals, and also available for manual audit and recount."

I very much hope that Council will have the wisdom to base its decision on this matter upon the opinions of experts such as Mr. Cates, Professor Schneier, Dr. Mercuri, and the authors of "The Secret Ballot at Risk"
report.

Yours sincerely and respectfully,

Michael Keefer

***

It is time to stop berating our City Councillors for researching and weighing information in order to make decisions which are in the best interest of the residents of our amazing city.

Please read the attached letter to elected officials. This clearly details the real issues around choosing to not implement on-line voting.

This has nothing to do with voter suppression and everything to do with security and ensuring that core democratic principles are upheld.

I quote "These core principles are:

1. Ensure only eligible electors can vote
2. Eligible electors can only cast one ballot
3. Each elector’s identity must not be linked to their ballot
4. Election results can be audited and independently verified
5. Security of the voting system is ensured"

The current situation with on-line voting does not uphold these principles.

Thank you to the 7 City Councillors who were courageous enough to make the right decisions on our behalf despite the baseless criticism.

Karen Phipps

***

Dear Mr. Mayor and Guelph's City Counselors,

I wanted to thank those of you who vote against internet voting and I hope you will continue to do so. It is clear to me, and to many, that internet security is a desire and not a reality. We see weekly headlines describing internet crime, scams and deceit. We've seen several incidents in the recent past of politicians or agents of politicians who have made efforts to deceive the public in order to steal votes and undermine democracy. The weakness inherent in the internet is a glowing target for the greedy. Choosing to support internet voting at this point in time is irresponsible and foolish and no amount of money or convenience saved can justify adopting it. The foundations of our democracy, with all its imperfections, has been weakened from within our country and from our neighbors to the south and I believe we need to be extra vigilant in our efforts to preserve it.

Thanks for listening (if you are).

Dave Withers

***

I have noted my household's support of online voting with my two city councillors Hofland and Allt who have told me that the majority in our area seems to be against it. I would just like to document our support FOR online voting with you. A household of four.

Hope you are having a great Easter weekend.

Gail Costigan

***

Dear Mayor and Councillors:

The Internet threat environment has changed since 2013 when Guelph did its initial analysis of online voting. Since then, Ontario, British Columbia, New Brunswick and the federal government have all released reports on online voting, and all have recommended against it at the provincial or national level. Threats have gotten worse while security technology has not advanced at the same pace, to the extent that the *Economist* magazine just did a cover story proclaiming "Why computers will never be safe".
http://www.economist.com/news/leaders/21720279-incentives-software-firms-take-security-seriously-are-too-weak-how-manage
http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security

Of course, decisionmaking is always about balancing risks versus benefits. I can tell you that when computer security experts examine online voting, they basically universally find that the risks are too high. See for example *Scientific American* from February 2016 https://www.scientificamerican.com/article/pogue-the-challenges-of-digital-voting/

If you do choose to continue with online voting, I urge you in the spirit of open government to conduct an open, public test of the full online voting system well in advance of the election, with permission for anyone around the world to remotely examine the system in detail for security vulnerabilities and to publicly report their findings. There is no security in obscurity.

In staff report CHR - 2013 - 30 "2014 Municipal Election: Methods of Voting", principles for a municipal election are outlined. Here is my evaluation of online voting against three of those principles:

- the secrecy and confidentiality of the voting process is paramount;

Use of a third-party vendor for online voting compromises voting secrecy and confidentiality. Even if the voting systems were developed and hosted in-house, the information necessary to cast a vote (the voter identification) is extremely difficult to completely separate inside the computer from the vote cast. Additionally, unsupervised remote voting opens the potential for anyone to view a vote that is being cast (and indeed to coerce the vote, or to pay someone for their voting credentials).

- the integrity of the process shall be maintained throughout the election;
- there is to be certainty that the results of the election reflect the votes cast;

The chain-of-custody for an Internet ballot extends from the personal computing device, across the Internet, and through to the voting servers. There are potential threats to the integrity of the process at every stage, from compromised ("hacked") home computers, through to denial-of-service attacks and potential vote alteration or addition of votes ("ballot stuffing") at the server end. Or the computer code could simply have errors in it (all computer programs have errors). There is no way to observe the entire process; it is a black box. Therefore there can be no real certainty that the results of the election reflect the votes cast.
Additional information supporting the above statements is available in an appendix to this email.

Thank you,
Richard Akerman

Appendix

Changes since 2013 report

The primary report is the July 16, 2013 "An Analysis of Alternative Voting Methods". http://guelph.ca/wp-content/uploads/AnalysisOfAlternativeVotingMethods.pdf

Both Elections Canada and Elections Ontario have been actively exploring the prospect of implementing an online voting channel for a number of years and have since allocated resources to undertake a detailed investigation and feasibility review of doing so.

As of 2017, neither Elections Canada nor Elections Ontario has implemented online voting, nor are they actively exploring the possibility.

A consultation by the Canadian Parliamentary Special Committee on Electoral Reform recommended against online voting[1], and the Canadian government accepted the recommendation.[2] On March 2, 2017 Elections Canada released an RFP which included the statement "Elections Canada has no plans to introduce electronic casting or counting of votes. Polling places will continue using paper ballots, marked and counted by hand."[3]
Ontario's Alternative Voting Technologies Report, released June 2013, recommends against online voting and there is no online voting in provincial elections in Ontario.[4]

[1] December 2016 – *Strengthening Democracy in Canada : Principles, Process and Public Engagement for Electoral Reform* – http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=e&Mode=1&Parl=42&Ses=1&DocId=8655791&File=291#87 – "Recommendation 4: The Committee recommends that online voting not be implemented at this time."

[2] April 2017 – Government Response to Report *Strengthening Democracy in Canada : Principles, Process and Public Engagement for Electoral Reform* – http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=e&Mode=1&Parl=42&Ses=1&DocId=8853290 – "The Government accepts this recommendation. We will not implement online voting at this time."

[3] March 2017 – Elections Canada RFP – https://buyandsell.gc.ca/cds/public/2017/03/02/967d72343b6234a0571287c709b7ae1f/ecrs-rfp-16-0167_-_anpp_-_ec-vsm-pppe_-_bilingual.pdf – "Elections Canada has no plans to introduce electronic casting or counting of votes. Polling places will continue using paper ballots, marked and counted by hand."

[4] June 2013 – Alternative Voting Technologies Report – Ontario Chief Electoral Officer's Submission to the Legislative Assembly (PDF) – http://www.elections.on.ca/content/dam/NGW/sitecontent/2014/reports/Alternative%20Voting%20Technologies%20Report%20%282012%29.pdf – "At this point, we do not have a viable method of network voting that meets our criteria and protects the integrity of the electoral process."

Additional Context

In fact, there is no provincial online voting anywhere in Canada, and there is only municipal online voting in Nova Scotia and Ontario. Reports from Nova Scotia [5], New Brunswick [6] and British Columbia [7] have all recommended against provincial online voting. Quebec has had a moratorium on provincial online voting since investigating problems with its electronic voting machines in 2005.[8]

[5] Elections Nova Scotia: Annual Report of the Chief Electoral Officer April 1, 2012 – March 31, 2013 (PDF) – https://electionsnovascotia.ca/sites/default/files/ENS%20AR%20Web%202012_13.pdf – specifically pp. 14-16 Appendix I: Internet and Telephone Voting in Nova Scotia.

[6] March 2017 – A pathway to an inclusive democracy (PDF) – http://www2.gnb.ca/content/dam/gnb/Departments/eco-bce/Consultations/PDF/PathwayToAnInclusiveDemocracy.pdf – specifically pp. 20-21 E-voting

[7] February 2014 – Independent Panel on Internet Voting: Recommendations Report to the Legislative Assembly of British Columbia (PDF) – http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

[8] October 2006 – Electronic voting – Le Directeur général des élections du Québec (DGEQ) – http://www.electionsquebec.qc.ca/english/municipal/media/electronic-voting.php
There is a consensus statement from US computer scientists advising against Internet voting.[9]

[9] http://usacm.acm.org/evoting/category.cfm?cat=30&E-Voting - "At the present, paper-based systems provide the best available technology...."

***

Ever since I witnessed voters (as a scrutineer) at a Guelph highrise descending from their apartments on Woodlawn Avenuue confused and distraught about having been phoned with erroneous advice about location of their polls, I have been very aware of the sanctity of our system of voting. As a result of this experience I attended Michael Sonia's trial, which, as we know never explained this event.
Now I am opposed to online voting as it is not as efficient as the regular method, for several reasons, one of which would be failure to allow for a recount of ballots, as there are no ballots with the online alternative. Another good reason is the lack of security in a system that I understand could be hacked by a fourteen year old.
So I implore you to please vote against changing our present system!

Yours truly
Elizabeth Macrae

***

April 18, 2017

Mayor Guthrie and members of Guelph City Council,

Re: Lack of security for Internet Voting

Sent by email.

Please include this letter in the council package for the next City Council meeting.

By way of explanation, In 2011 I was a victim of the Sona robo-call fraud. My privacy and my right to vote are very important to me and this incident shook me to the core. I registered a complaint with the government. In the following federal election, my name seemed to disappear from the voter roll. I received little satisfaction or assurances from the government that there would not be a future problem.

I sat in the courtroom at the sentencing hearing of Mr. Sona and distinctly heard the judge say that he did not believe that Mr. Sona acted alone. Yet no further prosecutions have taken place. I consider this event unresolved and the conviction of Mr. Sona has done little to reassure me.

I have spent considerable time reading about internet fraud and electronic voting fraud. My informal research has not allayed my fears and has left me with a healthy distrust of electronic voting.

There have been so many incidents of electronic hacking in the United States and around the world as well as in Canada. The number of fraudulent telephone calls and emails are growing exponentially. Software giants like Microsoft and Facebook release security updates on a continuous basis. My son's Sony account was recently was hacked as well. How can the city possibly afford this service to secure on-line voting?

For these reasons, unless the City can provide me with **absolute** assurances that my privacy will be maintained and that my vote will be secure, I **do not** support internet voting at this time.

Yours, truly,

Margaret Carter

***

Hi Dan and Bob,
Online voting should and must be a non-partisan issue, our democracy demands that we stand up for the best and fairest vote possible.

The world may never be ready for internet voting. When I ran in the last Federal election it was very interesting, those over 40 thought internet voting was a great, simple way to vote, those under 30 unequivocally thought it was crazy. They believed that online voting is far too insecure and easily manipulated. All voting online is absolutely hackable if someone is intent on manipulating the tallies and results. Nothing online is secure. Democracy is tenuous and precious and we need to protect it, and not allow petulance to get in the way of ensuring the voices of the people are fairly heard.

We can find solutions that work to ensure everyone who wants to vote can vote, but online voting, like Yahoo!, Best Buy, the DNC, and many other examples show that there is no such thing as security and privacy online. As my representatives at Guelph Council, please support the need for safe and secure voting by ballot.

Andrew Seagram

***

I would ask the city councillors opposing e-voting to continue their stance. I would ask those previously indicating that they were in favour to reconsider and vote against.

I have asked my daughter to send this email for me. I do not have a computer or access to one.

I am 87, live alone, do not drive and use a walker - obviously I have accessibility issues. If I could not make my way independently to the polling station to vote I am aware there are many options for me to get there OR to appoint a proxy OR other options such as having the Deputy Returning Officer come to my home to register my vote. There are advance pollls.

After discussing with my tech-savvy grandchildren I am concerned about the security of the vote. I am also concerned about the validity of the voters' list. I remember the days when the list was compiled by enumerators and copies were posted in neighbourhoods so that the list could be validated. The list based on MPAC is faulty.

I have asked a number of friends, acquaintances and neighbours for their opinion on the issue. Many are unaware of the discussions citing the lack of a daily newspaper, no access to computer, etc. They are also concerned about online voting but are unsure how they can express their opinion. The Mayor says to email but there is a large number of us who do not have that capability!

Thank you for your attention to this matter

Glenna Fryer

***

Hello Cam and all members of council,

I would like to send this email in support of keeping online voting. Online voting allows EVERYONE to vote, people who are unable to physically go to a polling station are able to vote from an accessible computer or electronic device. If online voting was taken away, accessibility would be lost for many individuals, yet their vote is just as important as the person who goes to a polling station. We should be increasing accessibility, not decreasing it. For those councillors who wish to abolish the online voting, please consider changing your opinion and stand up for accessibility.

Thank you,

Inderjit Arora

***

The Tribune printed a letter to the editor from me about ten years ago advocating online voting. It outlined the many benefits of online voting that people discuss today and pressed for progress, encouraging our electoral process to catch up with other processes such as banking, embracing online reach and increasing efficiency. Understanding that change grinds forward slowly on some issues, I accept that it took a decade for online abilities to finally be implemented in our last advanced election. However, it is truly disappointing that some of our leaders are recommending that we step back into old processes.

We all acknowledge that corruption and disruption can occur in all aspects of lives but we know the benefits of progress far exceed the risks of abuse as long as we diligently mange the processes to mitigate risks. I implore you to support Guelph's transition to online voting now.

Your role is not to resist and delay inevitable technological process but to support it. Lead us into the future rather than chaining us to the past. Vote for online voting.

Thank you

Ben McCarl

***

greetings! please include the following letter in Councillors' packages, thank you!!
I understand that Council will make a decision at next Monday's meeting about Guelph's option for online voting for the next city election.
I encourage Councillors to continue offering the option of online voting as it impacts myself & many others in the City.

as a person who lives with a disability that can flare up without any notice & leave me unable to leave my home, the option of online voting gives me access to voting if a severe flare up would happen.

one of the many things I love about the City of Guelph is the commitment to accessibility in all forms - online voting is truly a barrier-free option!

I look forward to hearing that you have all passed the motion to have the option of online voting on the next election!

from an almost 40 year resident of Ward 1 & a 46 year resident of Guelph!

Marlene Pfaff

***

Dear Mayor and Members of City Council
I was one of the many people in the city of Guelph who received a misleading robo-call during the 2011 federal election, telling me that my polling station had been changed and directing me to a place where there was no polling station. As you can imagine, I was confused and worried, but after much anxiety thankfully ended up at the correct polling station and was able to cast my vote.

When I heard on the news about the attempt to suppress voting, I was shocked and angered. Voting is one of the cornerstones of democracy and the idea that some political party would deliberately try to prevent me from voting so their own party could win still resonates as repugnant and deeply immoral. As you can imagine, I was also one of the many people from Guelph who contacted Elections Canada about my experience in the election.

Now we are facing the question of internet voting and given the number of scams, hoaxes and outright criminal activity on the internet, I think such voting is ripe for further voter suppression. No matter how many precautions the City takes, anti-democratic elements will try to, and sometimes succeed at, overcoming them on a far greater scale than the ignominious voter suppression of 2011 for which Guelph is now dubiously famous.

Does the city of Guelph want to be known as the place where democracy died? Even with the best intentions of City Council, internet voting could be the catalyst for this to happen. Voting in person stands the test of time and is still the greatest bulwark we have against voter suppression and for exercising our democratic rights.

Regards,

Jennifer Sumner

***

Hello,

Since I am unable to make the meeting I would like you to share this with the Councillors and Mayor.

I am strongly in opposition of online voting or any proximity of it. It is a road laden with traps, vulnerabilities and ultimately becomes a road where people distrust the results. This is a terrible road to go down..look at what is going on in the U.S. As a result of online voting, not to mention those out west outraged by their experience. Stick with manual counting and manual voting - there's no other way and venturing down the slippery road of online voting is a waste of time and energy.

The time and money people think they will save with online voting will become a quagmire of distrust and that in the end will cost much more time and money. Move on to more important challenges and leave this in the dust.
Thank you,

Marsaye Treen

***

Hi,

I recognize that there are challenges and risks with Online voting, but maintaining the change is necessary. Removing online voting sounds like an overreaction to the general fear of hacking, which is ill informed and unrealistic. I am appreciative that we have a city council who wants to modernize our democracy and improve accessibility to voting. I would challenge anyone who says we shouldn't move to tampering to provide credible evidence that it's a realistic fear, in a way that isn't riskier than someone conning the paper system by finding a way to vote multiple times over paper ballot.

In other words, please don't let council be overly cautious without well informed reason. Would their preference be we revert to needing everybody to show up in a room and have their hands counted? I doubt it. So let's accept that their is some risk, that the risk threshold of online voting is tolerable, and move on to more important issues like food insecurity, affordable housing, living wage and ranked ballots.

Robert Routledge

***

To the attention of City Council.

I have followed the public discussion about internet-enabled voting. I think there are several very troubling aspects to the proposal.

Since the end of door-to-door enumeration, Canadian voters' lists have been of dubious quality at best. Relying on computer-generated enumeration is bad; using those lists for internet voting will be worse.

I have heard the argument made that Internet voting addresses disability issues. In fact, I think it is quite the opposite. Polling stations should be accessible! For voters who have difficulty getting to the polls, the ballot box should be brought to the voter. I fear that if Internet voting is approved, it will be used as an excuse to do exactly the opposite! People will say, "Why should we waste money making the polling station accessible? Disabled people can just vote online!"

The comparison sometimes made between online voting and online shopping/ online banking is not valid. In an online banking transaction, for example, the essence of the transaction is to verify identity repeatedly, at every stage in the process. It's my bank account. I can look at it before and after the transaction and know that the transaction was made properly. If improper transactions are made, I will notice them. Voting is exactly the opposite situation. The key is to make sure that the vote is private and anonymous. So you can't have the same level of verification of identity.

The voting booths is a private sanctuary. No one can enter the voting booth while you're in it and no one can see how you mark your ballot. That didn't simply happen; it took years and decades of struggle to achieve that right. It is lost with Internet voting. No one can verify that votes are cast in private. A man who intimidates his wife, or a parent who intimidates a teenager, can simply stand over the wife or teenager while she or he casts her or his ballot. What can the wife or teenager do about that? The parent may have the only computer in the household, or to the parent may simply demand that the teenager vote in front of them. I can't see any way to ensure that this is not happening. It's a fundamental breach of the privacy of voting.

For all of these reasons, Councillors, I urge you not to support Internet voting.

Respectfully yours,

David Josephy

***

Hi.
I think online voting should stay. Here's a few reasons why I believe that:

1 - Accessibility. My girlfriend has bipolar disorder (was a patient at Homewood) and with that comes severe anxiety and generalized depression. On the best of days answering the front door is an easy way to fire off the anxiety. It's hard for her to go out as well. Having an option for online voting means she doesn't have to get extra anxious about voting.

2 - Security and safety. The opposing councillors have this list of demands that online systems fail to meet. And that there's no way to fully guarantee that an online system is secure and safe. By their standards analogue voting would also fail.

3 - Susan Watson. These councillors keep quoting Susan Watson who said (paraphrasing) that digital voter fraud is highly likely and gives the Robocall scandal as an example. This is the perfect example of why online voting should exist. A) It affected analogue voters, B) if voting online was a thing this scandal wouldn't have happened because people wouldn't have been misdirected to a non-existant polling station, and C) this wasn't voter fraud, it was voter suppression committed by the Harper government.

4 - if MPAC is so hugely terrible and Guelph's voter lists are so wildly out of date and inaccurate (as they claim) how is that acceptable for analogue voting. All the technical problems they have with the software are just that. They are problems whose solution is a little bit of money. There is no reason the voting system could be hardened by Oct 2018 (as someone who builds these types of systems daily and in much shorter time frames, I think I can authoritatively make that claim). All the problems they've listed off for the digital voting are all applicable and currently exist as problems for the analogue voting.

I know it's probably hyperbolic to suggest voter suppression, but their reasoning is misleading and reeks of fear-mongering. Both of which are used as tools for voter suppression.

Thank you for hearing me out.

Cheers,

Derek Kinsman

***

Dear Mayor Guthrie and Members of Council,

When this issue came before you recently, I was a solid supporter of e-voting; so much so, that I rebuffed efforts to be recruited to lobby against internet voting.

My position in favour was softened by reading the materials Ms. Susan Watson provided to Council's Committee of the Whole, and firmly reversed by reading Mr. Cameron Shelly's excellent summary of research on the topic in his April 11 letter to you, and by following up some of his research.

I urge you to read Mr. Shelly's letter attentively. I believe he has beautifully listed all of the advantages of internet voting (who would NOT favour e-voting for all those reasons!), before establishing to my skeptical and research-savvy mind that e-voting is not as yet sufficiently secure for use in Guelph.

I further urge you not to think of this as, or make this into, a partisan issue in your public debate. There is no logical connection between the core values of either the Left or the Right and a position either in favour or against e-voting. After all the Farbridge Council first brought us internet voting, and this second round is shaping up a preference on the Right.

Dennis Galon

***

Hello,

I'm writing to register my opposition to the online voting option for municipal elections. I believe the recent committee vote to go back to in-person paper ballot voting was the correct decision.

In the last election I voted using the online option. At that time I instantly saw the opportunities for easily voting on behalf of other family members. I didn't take advantage of those opportunities but my training in engineering has taught me to recognize flaws and potential problems even before they occur. The major flaws, as I see them, are the potential for:

1. Voting on behalf of apathetic family members or friends who choose not to vote

2. Coercing/forcing others (spouse, children, etc) to vote the way you want them to

3. Paying acquaintances or strangers for their voting information and voting on their behalf

The worst part about online voting's potentials for abuse is that they are inherently undetectable and as such there is no way to know if any irregularities happened or not in the last election. The fact that we don't have evidence of fraud is in no way indicative of its absence.

It may be true, as online proponents argue, that no system is perfect and there are opportunities for abuse of any system, but the online system's flaws are much easier to exploit and much harder to detect. That makes it clearly the inferior choice.

That said, the online system does make voting more accessible, and we need to examine and implement ways to make in-person voting similarly accessible, but not at the expense of vote integrity and security.

Regards,

Steve Mercer

***

I am in favour of access to online voting in the next election of City Officials.

Charlene Dwyer

***

I say YES to online Voting.

Mark Kenny

***

Hello. I would like to add my voice to the online voting debate. There is no cause to discontinue it. It helps a lot of people be able to participate in the voting process, which in turn allows for a better election result, that actually better reflects the opinions of the city residents.

Thank you

Heather Burke

***

Dear Mayor and Councillors,

I am writing to ask you to vote against instituting a system of electronic voting for Guelph elections. I do understand its advantages, particularly that it makes voting easier for seniors and others who have mobility issues. However, we can easily take steps to make sure that such people know they have the right to have a returning officer come to them, and that most campaigns have volunteer drivers ready to deliver them if they want to go to the polling station instead. I just don't think the advantages outweigh the risks. There is so much evidence out there that electronic voting is easily manipulated and subject to fraud. We may think these things won't happen at a municipal level, but we have, sadly, already seen that Guelph can be targeted for unethical electoral manipulation (the Pierre Poutine robocalls). Please consider voting against electronic voting in Guelph.

Sincerely,
Meg Thorburn

***

It's extremely important for accessibility to allow electronic voting. It's 2017, not 1917.

Thank you.

Amy Skeoch

***

I am a 32 year old citizen who groans when I have to wait in line to vote. I use the internet on a daily basis for all kinds of things I would like kept secure.

However, I would like to register my support for the council members in their finding that online voting should NOT be used in a Guelph election.

I find the many public appeals on social media and online by the mayor to be inappropriate behaviour from the position of mayor. Asking citizens to personnaly email councelors along with condemning "The Seven" for suspending the rights of

Guelph citizens is out of line, and a bad example of how our council, and mayors position should function. I also do not appreciate the mayor using examples like "hard working single mothers", or "people with accessabilty issues" to push a political agenda even if he genuinely thinks online voting is a good option. Have a referendum on the ballot instead of Tweeting about it.

One persons opinion on what should change does not make that the correct opinion, nor the correct change to make, not a change that everyone wants. There are opportunities for votes to come in outside of election day already.

As someone who only gets ONE VOTE in a small city for our civic positions of power, I am FOR taking EVERY measure to have extremely accurate vote tabulation. Any expansion of the system, unless PROVEN to make it MORE secure would be a downgrade for me.

Thanks.

Kris Kenney

***

I support council putting on line voting in place

Gary Roberts

***

Hello,

I was one of the 12,000 or so people who used online voting in the last election. This is something I would recommend and ask that you keep. It was not only extremely easy, but it also made me want to vote because I could do it convinently from my home, instead of having to go somewhere to vote. I am sure that this feature will help many people in Guelph who are low income and do not want to pay $6 on the bus to vote, those who are disabled and would prefer to do it from their homes, and those that are too lazy to go out and vote. Everyone should have their voice heard, and you should give them the channels to hear them.

Thank you,

Kayla McKay

***

Hello, although I have never needed to vote online I believe it is a valuable service that needs to remain available. As a person with anxiety I never know when I'm going to have an episode and would hate to miss out on my opportunity to vote because I can't bring myself to go out in public. Thank you for considering the feedback from city residents. I hope to hear good news about the fate of online voting.

Sabrina Moore

***

Simply, as one with a walking disability, please retain this form of voting for 2018.

Barry Smith

***

Dear Cam and members of council,

I would like to email to show my support of online voting. I believe online voting allows accessibility to those who may be unable to go vote at a physical location. Everyone should be allowed to vote and accessibility should not hinder them from voting. Please keep the online voting system, let everyone's vote be heard.

Thank you,
Devinder Ghuman

***

Voting online - Stay

Les Indoe

***

Dear whomever this concerns,

My family as a whole feels that the option for online voting for the 2018 election needs to stay in place!

Thank you for hearing our opinions

Sincerely

The Hendersons (Katie Henderson)

***

My name is Gary Langdon. I am in support of online voting.

***

Hi there....this is my vote for online voting yes please! (In response to Cam's fb post)

Thank you

Jenn Ephgrave

***

To whom it may concern,

I believe it is important for the city to keep the availability of online voting.

Please enter my opinion to your records.

Kind regards

Michael Chumbley

***

I truly believe this is the way if the future and an great way to increase voter turnout among younger voters.

Roxanne Eszes

***

Keep on line vote please

Stacey Roberts

***

Dear city councillors,

I think taking away this form of voting is very shortsighted and self serving.

This is not in this best interests of the people but in the best interest of a select few who would like to see this city return to the mayor of years past.

You will not gain more voters for your cause by doing this but you will drive more people to believe that public servants are only looking out for your self and not the public. This option is the way of the future and how to engage more people. All options have issues for fraud and instead of dropping this option more should be done to put security in it if it really is an issue. I don't believe fraud is an issue at a city election level but to each there own.

Please keep this option.

Thanks,

Jesse Clark

***

Greetings,

I am in favour of online voting.

Regards,

Miki Grosz

***

Please note I have had all my family living here. That was 7 voting 18 year olds.

I take them to the polling station and teach them their civic duty.

As the home of the conservative robocalls and a citizen who was called I reject online voting

Maria Berardine

***

Please keep online voting for 2018 election.

Jennifer McFadden

***

As a Guelph citizen I am asking that you please keep online voting available.   There are many in our community that have issues with accessibility and this is a great fair option and it is convenient for all.

Thanks

Leanne Stultz

***

I humbly ask city council and the mayor to please consider the vast amount of research and expert opinion that online voting is not a secure option at this time.
Laurie Garbutt

***

To whom it may concern,

I think online voting is a valuable thing to have for a couple reasons. It can help people with accessibility issues. It can increase the opportunity for busy people to vote. It saves paper, gas, and time in polling stations.

And also, it's 2017, why not vote online?

Daniel Bell

***

It has been pointed out that voting by internet is insecure. I do not want my vote wasted and need a secure, recorded paper ballot.

Jane Rodd

***

I am in support of Electronic Voting. If the Voters List is inaccurate, it will apply to both electronic voting and voting by paper ballot. There opportunities for fraud with both systems.

In the end, electronic voting allows people who may physically have trouble getting to the polls the opportunity to vote.

Yours truly,

Susan Moziar

***

.........for online voting.....especially for we seniors!!!

John Cunningham

***

Online voting should not be used in municipal elections in Guelph. Voter lists are grossly inaccurate, opportunities for voter fraud are enormous and voter anaunimity is impossible to achieve. With current levels of technology, electronic voting in Guelph should not be used in municipal elections.
Sincerely
Norm Bazinet

***

Hi,

I am writing to you to urge you to endorse the April 3 recommendation of the Committee of the Whole, which is to not pursue online voting for the 2018 municipal election.
As has been stated so eloquently by Professor Emeritus Michael Keefer in the Tribune of Thursday April 20, online voting does away with "the right to cast a secret ballot", which "in a public election is a core value".

It also opens the door to the very real possibility of election fraud. One hears regularly about people's online bank accounts being compromised, their credit cards charged with purchases that they haven't made, and personal information being stolen from companies such as Yahoo and Target.

If the banks, that are in the business of keeping people's money secure, are unable to guarantee the integrity of their customers' accounts, what hope is there for a municipal government to guarantee the security and integrity of an internet voting system?

In the recent Dutch election, old-fashioned hand counting of ballots was used to ensure that the election results were verifiable and were not tampered with in any way.

The most important aspect of the discussion regarding online voting in the next municipal election should be the integrity of the election results. According to many experts in the field of internet voting, at this point in time the possibility of election fraud is very real. Therefore I encourage you to NOT support internet voting for the 2018 municipal election. The integrity of the 2018 election and Guelph's subsequent municipal government depend on it.

Respectfully,

Monique ten Kortenaar

***

Dear Councillors,
I am 100 % in favour of voting online for elections. I have a relative with social anxiety. He has never visited a polling station to vote. BUT in the last municipal election he voted online!! Please be considerate of those with mental health issues and who are already marginalized in society. Please enhance accessibility for all our citizens. Thank you!!

Jane Moore

***

I fully support online voting. It's 2017. I can't believe this issue is up for debate.

Thanks. Trevor Favaro

***

Please keep online voting as an option. Just fix the security issues you're worried about. Don't take a step backwards in democracy.
Respectfully,

Stacy Cooper

***

I am in favour of providing residents the option of online voting.

Regards,
Jason Rice

***

Attention Clerks

I am not in favour in online voting at this time. I believe we have supports as needed for those not able to vote easily. I also believe we ensure democracy by showing up.

The online voting method is not 100% secure at this time and there are many in Guelph that would cheat. Remember we are the center of Robocalls and I was actually one household called.

Sincerely
Mark Berardine

***

I like online voting option for the municipal elections.

Ashley Richardson

***

I am in favour of online voting.
Kelli Rice

***

Hi

I would like to voice my support for the online voting option in Guelph.

Regards,

Scot Barlow

***

To the Honourable Cam Guthrie, Mayor of Guelph and Members of Guelph city council,

My name is Sarah Parro, and I am writing to you about my experience with voter suppression.

When I became the legal age to vote in 2009, I was excited about voting. It was a responsibility that I deeply wanted to cherish and to become more involved in politics. The election of 2011 my house received a phone call that our polling station had been changed by Elections Canada. If it were not for my father who questioned the phone call, my entire household would have been hoodwinked out of voting that year. That form of voter suppression was successful with paper ballots.

Not only am I turned off of politics, I now look at voting very differently. I look at it like a chess game and that same year was the year that I questioned our democracy. After everything happened, my vote still counted because thankfully our household was not fooled. However, the primary topic is the idea of online voting. Look up the embarrassment of what was the 2011 robocall scandal; and then give the person responsible behind that plan a computer with digital codes to a list of voter information online.

Please understand my concerns and my plea to reconsider the advantages we have currently with the ballot system.

Thank you,

Sarah Parro

***

Yes, on line voting should stay.

Cheryl Sajkowski

***

Im concerned with the rush towards online voting.

I am an IT professional and have done several security overview contracts including one for Nuclear Safety Solutions, a consulting engineering firm that works with Bruce Nuclear Power as well as one for the CBC.

I am extremely aware how difficult proper security can be, especially within a restricted budget. There is great incentive to tamper with elections at all levels of government.

We have seen this in the USA before, with major issues with Diebold voting machines (unforunately, some of their products have appeared at other in-person elections in this city as well, as I noted). Please see

http://columbusfreepress.com/article/diebold-indicted-its-spectre-still-haunts-ohio-elections

and

"WATCH: Computer Programmer Testifies He Helped Rig Voting Machines"
http://www.mintpressnews.com/214505-2/214505/

and

https://en.wikipedia.org/wiki/Hacking_Democracy

If you were to conduct online voting, an openly auditable ledger should be available to ensure vote counts are legitimate. Shared public ledger aka blockchain technology could assist in this regard and make it harder to attack the online voting process.

Unfortunately, none of the promotion of online voting mentioned any of the specifics of the security undertaken to ensure legitimacy of the vote count, nor any awareness of the diebold history, or emerging systems such as blockchain technology (which Wall Street is moving towards to provide complete transparency and fairness to many of their processes).

It seems it is a rush into online voting and I do not think we are properly prepared for this.

I'd like to thank the Mayor's outreach on Facebook for reminding citizens to weigh in on this issue, otherwise I might have forgotten.

Ken Chase

***

Requesting online voting continue to be an option in upcoming elections.

Deby Smith

***

Dear city clerks,

Please include the following to the agenda addendum for the discussion on internet voting.

Sincerely,
Yves Younan

Dear Mayor Guthrie, Council Members,

As a computer security professional who has spent more than ten years both in the academic computer security space as well as in industry, I would like to voice my opposition to internet voting. While I am a strong believer in any system that would help improve voter participation, I do not believe that the increase in voter participation that internet voting may bring is worth the risk of supporting internet voting.

I received my PhD from the Katholieke Unversiteit Leuven in Belgium, where my research focused on mitigating common vulnerabilities in today's operating systems. After completing a post-doc at the university, I worked at both a large Canadian mobile phone company as well as a large security and networking company where I have focused on finding vulnerabilities and helping fix them. My current role is to manage an international group of researchers dedicated to finding vulnerabilities in third-party products and helping vendors correct these issues.

A major problem with internet voting is that currently it would be extremely hard to ensure the security of the process: not only are the devices at risk themselves, but so are the voters. In the case of devices, hackers spend considerable resources finding vulnerabilities that are not disclosed to the vendors which could be used to break into these devices and change vote tallies. While it is clear from recent news that nation states are capable of influencing elections of other nations through cyber attacks, it is not outside of the skill set of a lone hacker to influence a local election. While electronic voting devices that are not networked can also be hacked, it is much harder to perform such an attack as a hacker would have to gain access to every one of those devices physically. This is not the case with internet voting where all devices are connected to a network and an attacker can launch these attacks from thousands of kilometers away.

Next to potential vulnerabilities in the devices used for an election, one has to also worry about the security of the computers that voters use. It is not unheard of for hackers to control millions of home computers for a single purpose. A targeted campaign aimed at a local population could be successful, especially in close elections where the difference in votes could number in the dozens or hundreds. This is also where voting differs significantly from internet banking: if a bank customer is compromised and an unauthorized transfer is made, there is a clear paper trail and the customer will eventually notice and the problem can be remedied at a later date. If one hundred customers are compromised, the bank fraud detection system will kick in, since the activity is anomalous. Voting is different: it is not an activity that happens every day, so building a history of regular vs. anomalous behaviour is much harder. Additionally, if one hundred voters vote for a certain candidate, who is to say this was not the intent of those voters? Given the issues with voting secrecy, it is also not possible for a voter to go back and verify that their vote was cast correctly. Even if this verification was possible, most voters would not do this and if they did the verification from their compromised computers where their vote was originally changed, they could still end up seeing what a hacker wants them to see.

The issues above are important issues to consider when allowing internet voting and while I focused on vote changing issues these are not the only problems. There are also potential issues with denial of service attacks, where attackers disable internet connectivity to either the voting devices or to certain users. If hackers were to break into the website of a candidate they oppose, they could subsequently look at the internet addresses of the voters visiting that website and on the day of the vote try flood the internet connections of those voters. In a close election, this could again be enough to influence the result. This type of attack doesn’t even rely on the security of the voting devices or that of the voters but the website of a single candidate.

Given the many potential issues, I believe internet voting should be avoided.

Sincerely,
Yves Younan,

***

Dear Clerks Staff;

I would like my opinion known on the upcoming City Council issue of online voting in Guelph, as follows:

Overwhelming evidence worldwide clearly shows that cyber hacking of computer systems is increasing in sophistication and will outstrip every effort to block it. It is therefore highly irresponsible to commit any voting methods to online systems.

Democracy must be protected, and the voting booth - with physical, reviewable data - must be maintained.

There must be NO online or purely digital voting systems in elections held in Guelph - or anywhere in Canada - whether federal, provincial or municipal.

Sam Turton

***

I wld like online voting, thx

Shelly Martin-Ganson

***

I support on line voting

Jim Rooney

***

What follows is my letter to the editor, which appeared in the Guelph Mercury Tribune, concerning the Mayor's response to Guelph City Council's recent e-voting decision. I believe that vote was appropriate, and trust that the decisions of individual Councillors on both sides of the debate were based upon their judgement of the security concerns, not petty partisan interests as the Mayor has charged.

"THANKS #GUELPH! IT'S CLEAR, THE CITIZENS WANT ONLINE VOTING TO STAY! PLEASE SHARE!"

Thus blares the heading of a piece that appeared on Mayor Cam Guthrie's blog the morning of Wednesday, April 5 (the day I encountered it). Immediately beneath that was a text graphic almost large enough to fill the screen of a typical laptop, saying:

"What you allow is what will continue."

Reading this far I was intrigued, but also confused. What exactly is this sentence intended to imply, I wondered. "You" must refer to Guelph voters, presumably. The tone is one of admonishment. Apparently our mayor thinks we've been "allowing" something sinister to go on, and unless we Guelphites rise up in opposition to it, it will continue. And whatever it is has something to do with online voting?

Never known for my patience, I scanned toward the bottom of the page where I knew to expect a summary of the main point. What I found there was a list of the names and email addresses of the seven City Councillors who recently voted against implementing online voting in Guelph for the 2018 municipal election. The text beneath that list ended, "... our ability to make voting accessible for all is under attack! Thank you again Guelph for standing up and speaking out!"

I was taken aback by this. Was the mayor actually accusing seven separate City Councillors of opposing e-voting for reasons other than the security concerns they cited? Of course I went back and read the mayor's missive through from the start. Sadly, the experience was not reassuring. The view expressed seems jaundiced to the point of paranoia. One particular sentence stands out:

"The majority of the citizens of Guelph are not buying into the vocal minority who are instilling fear, unfounded conspiracy theories, dangling 'what-if' scenarios and tactics that appear to try and suppress our citizens votes and voices."

Read that again: "... to try and suppress our citizens votes...." [sic]

Are we to understand that the greater part of Guelph's municipal representatives are corrupt, and to such an extent that they mean to suppress the vote? That's quite a charge! Not only is it facile and groundless, it's actually incoherent: what discernible personal benefit is to be gained by a vote against the e-voting proposal (or for that matter, for it)? Do only these councillors' detractors have computers?

Mayor Guthrie is issuing a very serious, very public accusation. Very serious, very public, and very unprofessional. If I were his lawyer I might be uttering, privately, an admonishment of my own. I'm quite sure I'm not alone in regarding the mayor's rhetoric as inappropriate. Guelph's councillors are our trusted neighbours, our often longtime acquaintances, sometimes our friends and relations. Needless to say, they are also the public servants who were put in office by virtue of our support. I'd say an apology is in order.

I will close with a few comments about the merits of the question itself. Although it usually comes as a suprise to the layperson (I was unaware of it myself) at the present time, credentialed computer scientists comprise the group most consistently OPPOSED to internet voting. That fact should give us — literally — pause, here in Guelph: before proceeding the City should, at the very least, slow down and give the question careful consideration, after consulting with experts in the field who have no vested interest in the decision being made.

A poll of public opinion regarding the security of internet voting (which was actually conducted) is, as a means of determining policy, of virtually no value at all. Why should we care what our own uninformed guess might be concerning the very technical security issues involved? This is the kind of question that cries out for consultation with impartial experts in the field. (Needless to say, voting system vendors don't qualify.)

Spurred chiefly by the Mayor's strident rhetoric, I have devoted quite a few hours over the past several days researching this fascinating, consequential subject. I am persuaded by that reading that the Council's vote in opposition to this proposal was a prudent and appropriate one. I would urge anyone interested in weighing the merits of the "no" position to visit verifiedvoting.org/resources/internet-voting

What you learn might surprise you.

Charlie Cares

What follows is a list of recent articles and documents on internet voting security culled from my web searches, with short extracts and links. I submit this information to Council in hopes of raising the level of discourse.

Internet voting is just too hackable, say security experts
USA Today
(2016-01-28)

Attempts in other countries seem to show that Internet voting only increases turnout negligibly. Efforts in Canada and Switzerland found that it only caused people to vote earlier but didn’t cause more people to actually vote, Smith told USA TODAY in an interview. She noted the federal government spent a decade and a half and more than $100 million on a demonstration Internet voting project for military personnel overseas that included a program called SERVE, the Secure Electronic Registration and Voting Experiment. It was shut down by the Pentagon over security concerns. "They just abandoned the effort," she said.

https://www.usatoday.com/story/tech/news/2016/01/28/internet-voting-not-ready-prime-time-security-risks/79456776/

VerifiedVoting.org
If I Can Shop and Bank Online, Why Can’t I Vote Online?

The sum of all of these considerations is simple. The security, privacy, and transparency requirements for online voting are much more complex and stringent than they are for E-Commerce transactions. The acceptability of small losses and the strategies for managing risk are very different between the two. And it is hard to grasp the full implications of the fact that online elections might be compromised and the wrong people elected via silent, remote, automated vote manipulation that leaves no audit trail and no evidence for election officials or anyone else to even detect the problem, let alone fix it. These ultimately are the reasons we cannot provide satisfactory security for online voting even though we can for online commerce.

https://www.verifiedvoting.org/resources/internet-voting/vote-online/

Gizmodo
Why Can't We Vote Online Yet?
(2016-10-27)

“Definitely, I think it’s not ready,” Avi Rubin, a professor of computer science at Johns Hopkins University and the technical director of the school’s Information Security Institute, tells me. “I don’t think it can ever be ready.”

Rubin has a problem with the approach of internet voting as a whole, not just the ways in which it might be carried out. “Computerized voting is not a good idea. It’s a nontransparent medium,” he says. “If voting was online on the internet, there’s going to be no way to prove it wasn’t [manipulated]. It’s not verifiable and auditable.”

http://gizmodo.com/were-not-ready-for-online-voting-1788124756

Internet Voting in Canada: A Cyber Security Perspective
(ERRE Committee submission)
Aleksander Essex, Western University
(2016-??-??)

... contemporary commercial Internet voting systems consist of a standard web - application framework; a voting program (typically Javascript) is sent from the election server across the Internet to your browser. When you cast a ballot, the information about your selections is returned to the server and stored in a database to be tabulated later. Security is required at all points in this chain: at your device, in transit, and at the election server. From a security perspective, this architecture introduces a host of potential threats not found in Canada's current in-person hand-counted paper ballot method.

... considerable concern about the safety of Internet voting exists among international technology and cyber–security experts. Echoing a statement by prominent U.S. computer technologists (Computer Technologists), we urge Internet voting only be adopted after the numerous technical threats outlined above can be suitably mitigated, and strong mechanisms put in place to prevent undetected changes. The entire system must be reliable and verifiable in a way that is convincing to the voting public.

http://www.parl.gc.ca/Content/HOC/Committee/421/ERRE/Brief/BR8610535/br-external/EssexAleksander-e.pdf

-----

Annual Report of the Chief Electoral Officer, Elections Nova Scotia
(2013-03-31)

... while most would agree that online voting is consistent with our increasingly online society, the basic questions of how to maintain the security, validity, and integrity of our elections has not yet, in our opinion, been satisfactorily answered. Until credible answers to these questions are available, and until functioning, transparent Internet and telephone voting systems have been demonstrated and proven, extreme caution and prudence is required.

https://electionsnovascotia.ca/sites/default/files/ENS%20AR%20Web%202012_13.pdf

-----

"Computer Technologists' Statement on Internet Voting"
(32 signers from various universities, corporations and government institutions, including Stanford, Princeton, University of Maryland, Indiana University, Carnegie Mellon, Yale, East Tennessee State University, UC Berkeley, Towson, University of Iowa, UC Observatories/Lick Observatory, Johns Hopkins, Purdue, University of Texas at Austin, Rice University, Software AG, SPARTA, SRI International, BT Global Services, IBM Research, Lawrence Livermore National Laboratory)
(2012-09-??)

Internet voting should only be adopted after these technical challenges have been overcome.... The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed to be free of malicious logic. [...] There must be a satisfactory way to prevent large-scale or selective disruption of vote transmission over the internet. [...] There must be strong mechanisms to prevent undetected changes to votes, not only by outsiders but also by insiders such as equipment manufacturers.... [...] There must be reliable, unforgeable, unchangeable voter-verified records of votes.... [...] The entire system must be reliable and verifiable even though internet-based attacks can be mounted by anyone, anywhere in the world. [...] Given this list of problems, there is ample reason to be skeptical of internet voting proposals. [...] The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

https://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf

-----

Pacific Standard (Santa Barbara, CA)
Why Can’t We Just Vote Online?
(2016-07-11)

If the ultimate goal is maximizing the country’s voting turnout, shouldn’t we develop an Internet voting system? Voting from a computer at home could be far easier than waiting in long lines at polling stations or filling out mail-in forms. But can it ever happen? “For as far into the future as I can see, the answer is no,” says David Jefferson, a computer scientist in the Center for Applied Scientific Computing at Lawrence Livermore National Laboratory. In May 2015, Jefferson examined the possibility of Internet voting in a paper called “Intractable Security Risks of Internet Voting.” For anyone who has ever owned a personal computer, the first problem is obvious: malware. “We’re not even remotely close to guaranteeing that there’s no malware on your computer,” Jefferson says. The malware can do whatever task it’s programmed to accomplish, from erasing votes cast to changing them. And they can do these things without leaving any trace. “The malware might erase itself a half second later, and so there might be no evidence. And that’s one of half a dozen of problems.”

https://psmag.com/why-cant-we-just-vote-online-16bae52e7b7e

The Conversation (Australia)
Election explainer: why can’t Australians vote online?
(2016-06-22)

... federally, the Joint Standing Committee on Electoral Matters has ruled out allowing Australians to cast their vote online, arguing it risks “catastrophically compromising our electoral integrity”. Despite years of research, nobody knows how to provide evidence of an accurate result while keeping individual online votes private. Internet voting is similar to online banking, except you’re not sent a receipt saying “this is how you voted” because then you could be coerced or bribed. Your vote should be private, even from the electoral commission. There are three reasons why Australia shouldn’t move to an online voting system:

the system might not be secure;
the code might not be correct; and, most importantly,
if something goes wrong, we might never know.

http://theconversation.com/election-explainer-why-cant-australians-vote-online-57738

Motherboard (Vice.com)
This Is Why We Still Can’t Vote Online
(2016-10-19)

J. Alex Halderman, professor of computer science and engineering at the University of Michigan, welcomed the opportunity to try to legally break into government software with his students. Within 36 hours, they found a tiny error that gave them full control of the system. "The flaw that we exploited was just such a small error—in tens of thousands of lines of computer source code, in one specific line the programmer had used double quotation marks instead of single quotation marks and that was enough to let us remotely change all the votes," said Halderman. To have a bit of fun, Halderman and his students did not alert officials of the their finding. Instead, they made modifications so that the University of Michigan fight song would play after a vote was cast. It took officials two days to realize there had been a hack, which spotlights yet another concerning element of online voting: a system could be hacked and, without a calling card like a university theme song, officials could be none the wiser.

https://motherboard.vice.com/en_us/article/this-is-why-we-still-cant-vote-online

-----

Daily Dot
Online voting is a cybersecurity nightmare
(2016-06-10)

But internet voting isn’t online banking or video calling or tweeting. Voting is a special activity, and trying to do it online poses special problems, most of which security researchers don’t yet know how to solve. “The technology is just too insecure to entrust such an important right of American people to that insecure technology,” said Bruce McConnell, global vice president and cyberspace program manager at the East West Institute and former deputy under secretary for cybersecurity at the Department of Homeland Security. [...] “We do not know how to build an internet voting system that has all of the security and privacy and transparency and verifiability properties that a national security application like voting has to have,” said David Jefferson, a researcher at the Center for Applied Scientific Computing at Lawrence Livermore National Laboratory...." "Unlike in banking, where fraud is detectable because money either lands in the appropriate place or disappears, and in paper voting, where physical evidence must be tampered with to rig the results, technology lets people do things while leaving literally no trace." "The system goes to great lengths to destroy the link between my name and the ballot that I cast," said Dill. "That's a property that's special to elections that almost no other system of electronic transactions deals with in the U.S. It is possible to hide evidence of tampering with paper ballots, but doing so is often clunky and requires a team of conspirators with access to far-flung physical resources. "The more wrong it is, the more noticeable that would be," said Mark Ryan, a computer security professor at the University of Birmingham. "That's a feature we don't have with computers."

https://www.dailydot.com/layer8/online-voting-cybersecurity-election-fraud-hacking/

Institute of Electrical and Electronics Engineers (IEEE)
The Security Challenges of Online Voting Have Not Gone Away
(2016-11-14)

Voting is an unusually difficult security problem, because officials must guarantee a correct result while simultaneously ensuring that voters' choices remain private—and all without being able to trust any individual participants to act impartially. Furthermore, the election has to produce a result on election day, and we cannot delay voting or rerun the election if the system comes under attack. These requirements mean that traditional online security techniques, like those used to protect banking and commerce, are insufficient for elections. [...] In light of the uncertain benefits of voting online, it is crucial that we in the United States not rush to entrust our democracy to it. Some of the most difficult unsolved problems in computer security stand in the way: authenticating remote users, protecting home computers from malware, safeguarding online communication, preventing denial-of-service attacks, and protecting critical infrastructure from nation-state attackers. These challenges are among the most exciting and important in computer science and engineering—and many are striving to address them—but it may be decades, if ever, before they are solved to the level that we can vote online with confidence.

http://cybersecurity.ieee.org/blog/2016/11/14/ieee-spectrum-tech-talk-the-security-challenges-of-online-voting-have-not-gone-away/

Stanford University
Why Online Voting Is a Danger to Democracy (interview with Stanford Computer Scientist David Dill)
(2016-06-03)

Q: Online voting could threaten the fundamental legitimacy of elections?

A: From the perspective of election trustworthiness, Internet voting is a complete disaster. While you can't stop all election fraud, elections must have a higher standard of credibility. They need to have the perception of being low fraud. If you have an election system where fraud can be committed and – this is very important – that fraud is undetectable, then you don't really have a reason to trust the outcome of the election. And that's very bad in a democracy, because the whole goal of an election is to satisfy the people who lost the election that they lost fair and square and that the candidate who is elected is legitimate. [...]

Q: Ultimately, is paper the gold standard we should stick to?

A: Yes. Paper has some fundamental properties as a technology that make it the right thing to use for voting. You have more-or-less indelible marks on the thing. You have physical objects you can control. And everyone understands it. If you're in a polling place and somebody disappears with a ballot box into a locked room and emerges with a smirk, maybe you know that there is a problem. We've had a long time to work out the procedures with paper ballots and need to think twice before we try to throw a new technology at the problem. People take paper ballots for granted and don't understand how carefully thought through they are.

https://engineering.stanford.edu/news/david-dill-why-online-voting-danger-democracy

-----

CSO (International Data Group - publisher of Computerworld, PCWorld and Macworld)
Hack the vote: Experts say the risk is real
(2016-09-08)

This is not tinfoil-hat conspiracy theory. The warnings are coming from some of the most credible security experts in the industry. Richard Clarke, former senior cybersecurity policy adviser to presidents Bill Clinton and George W. Bush, wrote recently in a post for ABC News that not only are US election systems vulnerable to hacking, but that it would not be difficult to do so. “The ways to hack the election are straightforward and are only slight variants of computer system attacks that we see every day in the private sector and on government networks in the US and elsewhere around the world,” he wrote, adding that, “in America's often close elections, a little manipulation could go a long way.”

http://www.csoonline.com/article/3116964/cyber-attacks-espionage/hack-the-vote-experts-say-the-risk-is-real.html

-----

Recode
Why you can't vote online
(2016-11-07)

You can bank online and shop online, but you can’t vote online. After all, transferring thousands of dollars with a click of a button should require more security than ticking a box on an electronic ballot, right? Wrong. Online banking works by heavily verifying users’ identities, but, by law, voting in American elections has to be anonymous, which greatly complicates verifying voter identification. [...] Before the system went live, the city [Washington, D.C.] ran a trial, asking researchers to attempt to break into it. “Within 48 hours of the system going live, we had gained near-complete control of the election server,” wrote the University of Michigan team who took on the challenge to pry into D.C.’s pilot program. “We successfully changed every vote.... [...] ... until there’s some radical new discovery in computer security, experts across the board say Americans’ best bet is to record paper ballots for the foreseeable future. The convenience is just not worth the risk.

https://www.recode.net/2016/11/7/13542220/no-online-voting-paper-ballots-hacking

-----

NPR (National Public Radio, US)
Vulnerable Voting Machine Raises Questions About Election Security
(2015-04-16)

Computer security experts have warned for years that some voting machines are vulnerable to attack. And this week, in Virginia, the state Board of Elections decided to impose an immediate ban on touchscreen voting machines used in 20 percent of the state's precincts, because of newly discovered security concerns.

http://www.npr.org/sections/itsallpolitics/2015/04/16/399986331/hacked-touchscreen-voting-machine-raises-questions-about-election-security

-----

The Guardian (London, England)
Why electronic voting isn't secure – but may be safe enough
(2015-03-30)

“... there are three requirements for robust political elections: security, anonymity and verifiability. “Meeting those three requirements is a very difficult problem quite unlike other transactions.” [...] “Online banking suffers problems but refunds are possible after checking your bank statement. You can’t ‘refund’ a vote and ‘vote statements’ can’t be provided to check your vote was correctly recorded as that would enable vote selling and coercion.” All that paper in standard ballots may seem old fashioned, but it leaves a trail that votes cast from PCs and phones don’t, agreed other experts. “There’s a fundamental conflict between verification and keeping votes anonymous,” Jim Killock, executive director of the Open Rights Group. “Paper ballots do this very neatly but computers find this hard because they leave audit trails." Voting away from polls raises the spectre of vote manipulation, explained Ross Anderson, a computer security professor at the University of Cambridge.

https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure

-----

Wired
America's Electronic Voting Machines Are Scarily Easy Targets
(2016-08-02)

More than half of the states conduct post-election auditing, by checking vote totals against paper records, to ensure that the votes are accurate. Both Smith and Norden agree that this sort of auditing is the single best way to guarantee confidence in election results, as does MIT computer scientist Ronald Rivest, who has written extensively on voting machine issues. The problem is that not every state does post-election audits. And even some that require them by law, namely Pennsylvania and Kentucky, don't actually use voter-verifiable paper trails, meaning they have no way to complete an audit.

https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/

Politico
Paperless voting could fuel 'rigged' election claims
(2016-09-07)

"Paper trails are absolutely essential with current security technology," said Alex Halderman, a computer science and engineering professor at the University of Michigan who has researched voting machine security. "It's a serious problem that there are these states that don't have any kind of auditable record."

http://www.politico.com/story/2016/09/paperless-voting-could-fuel-rigged-election-claims-227806

Politico
How to Hack an Election in 7 Minutes
(2016-08-??)

The appeal of such machines seemed plain: Voting was crisp, instantaneous, logged digitally. To state officials—and, at first, voters—the free federal money seemed like a bargain. To computer scientists, it seemed like a disaster waiting to happen. Wallach remembers when he testified before the Houston City Council, urging members not to adopt the machines. “My testimony was: 'Wow, these are a bad idea. They’re just computers, and we know how to tamper with computers. That’s what we do,'” Wallach recalls. “The county clerk, who has since retired, essentially said, ‘You don’t know anything about what you’re talking about. These machines are great!’ And then they bought them.”

http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144

House Subcommittee on Information Technology (United States Congress)
Written testimony of Princeton University Professor of Computer Science Andrew W. Appel
Hearing on “Cybersecurity: Ensuring the Integrity of the Ballot Box”
(2016-09-28)

I’m not the only one who’s demonstrated how to hack a voting machine. Colleagues and students and Princeton University and elsewhere have demonstrated the same principle on several different models. This is not just one glitch in one manufacturer’s machine, it’s the very nature of computers. And some voting machines can be hacked without ever touching them, by means of computer viruses transmitted on ballot cartridges.

So how can we trust our elections when it’s so easy to make the computers cheat? Forty states already know the answer: vote on optical-scan paper ballots. The voter fills in the bubble next to the name of their preferred candidate, then takes this paper ballot to the scanner—right there in the precinct—and feeds it in. That opscan voting machine has a computer in it, and we can’t 100% prevent the computer from being hacked, but that very paper ballot marked by the voter drops into a sealed ballot box under the opscan machine. That’s the ballot of record, and it can be recounted by hand, in a way we can trust.

https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Appel-Princeton-Testimony.pdf

-----

Chicago Tribune
Recounts or no, U.S. elections are still vulnerable to hacking
(2016-12-26)

"... paperless digital voting machines, used by roughly 1 in 5 U.S. voters last month, present one of the most glaring dangers to the security of the rickety, underfunded U.S. election system. Like many electronic voting machines, they are vulnerable to hacking. But other machines typically leave a paper trail that could be manually checked. The paperless digital machines open the door to potential election rigging that might not ever be detected. [...] If I were going to hack this election, I would go for the paperless machines because they are so hard to check," said Barbara Simons, a former IBM executive and co-author of "Broken Ballots," a history of the unlearned lessons of flawed U.S. voting technology.

http://www.chicagotribune.com/news/nationworld/ct-election-hacking-recount-20161226-story.html

-----

CBC Radio
U.S. voting machines are way too vulnerable to hacking
(2016-10-14)

"All of the touch screen voting machines that are in use today in the U.S. were analyzed about a decade ago in state commission studies in California, Ohio and Florida," Wallach says. "And what we found then is still true today … these machines have unacceptable security."

"It's unfortunately easy to compromise the machines to tamper with the votes," Wallach says. I asked him if they are more vulnerable than a personal smartphone. "The issue," he said, "is comparing voting machines to paper, right? It's incredibly difficult for a hacker on the other side of the planet to change a piece of printed paper."

http://www.cbc.ca/radio/day6/episode-307-voting-machine-hacks-life-on-mars-how-to-say-gif-detroit-graffiti-cholera-in-haiti-and-more-1.3801636/u-s-voting-machines-are-way-too-vulnerable-to-hacking-1.3801639

The Guardian of P.E.I.
Constantine Passaris: A more inclusive democracy
(2017-03-17)

At the outset, every Commissioner was of the opinion that the time had arrived for e-voting. [...] What changed the Commission’s mindset was the expert testimony that was overwhelmingly against proceeding with e-voting at this time. It became abundantly clear that the risks of throwing an election because of e-voting were too high. The experts emphasized that security, privacy and confidentiality could not be guaranteed under the current electronic infrastructure. Above all, the sacrosanct anonymity of who a person votes for at the ballot box, which is the gold standard for one person one vote, would be shattered by moving to electronic voting at this time. In consequence, the Commission made a cluster of recommendations on e-voting. It recommended against adopting e-voting at this time.

http://www.theguardian.pe.ca/opinion/2017/3/15/constantine-passaris--a-more-inclusive-democracy.html

-----

InfoWorld
If the election is hacked, we may never know
(2016-10-05)

In the absence of voter-verified paper records, getting at the truth of a vote will be difficult. Cynthia and Ernest Zirkle ran for the Democratic County Committee of Fairfield Township, N.J, in June 2011. It was a very small election, with fewer than 100 votes. This election used one electronic, touch-screen voting machine with no paper copies of the individual votes. Ms. Zirkle and her husband lost the election. But she knew the results were wrong, because she had a good idea about who had voted for her. Proving it took work. "There was no verifiable paper trail, or back-up paper to see if the names were reversed," said Ms. Zirkle, in an interview. What she suspected was true: The votes that the Zirkles should have received went to their opponents. The ballots were programmed incorrectly -- and testing prior to the election missed the problem. Consequently, Ms. Zirkle gathered affidavits from people who said they had voted for them. This was used to help convince a judge to order a new election. The Zirkles easily won their new election.

http://www.infoworld.com/article/3128078/election-hacking/if-the-election-is-hacked-we-may-never-know.html

-----

Bloomberg
The Computer Voting Revolution Is Already Crappy, Buggy, and Obsolete
(2016-09-29)

546 people had cast ballots. When he got an e-mail a week later with Shelby County’s first breakdown of each precinct’s voting, he ran down the list to the one precinct where he knew the tally for sure. The count for Unity Christian showed only 330 votes. Forty percent of the votes had disappeared. If you’re an election official, losing votes is a very big deal, but it presents a special problem in Tennessee. Most counties in the state don’t keep paper records of ballots, so there are no physical votes locked in a room somewhere, ready to be recounted.

https://www.bloomberg.com/features/2016-voting-technology/

Quartz
The global e-voting disaster: Why the US and the world shouldn’t try to make elections too high tech
(2012-11-06)

“It’s an odd situation to be in where the people who are being called luddites are engineers,” says Matt Blaze, director of the distributed systems lab at the

University of Pennsylvania. “In the case of electronic voting, you have this reversal of the normal roles where the people who are closest to the technology are warning that there might be some pitfalls you want to think carefully about.” That’s one reason why Germany’s highest court ruled electronic voting unconstitutional in 2009, and most of Western Europe has backed away from the practice. The same is true of most states in the US, where only six holdouts continue to allow voting on machines with no paper record as a backup. Those that do allow it are Georgia, South Carolina, Louisiana, Maryland, Delaware and New Jersey.

https://qz.com/24614/the-global-e-voting-disaster-why-the-us-and-the-world-shouldnt-try-to-make-democracy-high-tech/

Scientific American
E-Voting Refuses to Die Even Though It's Neither Secure nor Secret
(2016-10-31)

In 2012 Alaska became the first state to allow internet voting for all residents—roughly 740,000 people spread over about 1.7 million square kilometers. “The motivation to offer internet voting is a good one to make it easier for geographically dispersed people,” Epstein says. But just like military personnel overseas, Alaska online voters also give up their right to a secret ballot. “When returning the ballot through the secure online delivery system, your are voluntarily waiving your right to a secret ballot and are assuming the risk that a faulty transmission may occur,” reads a notice on the state’s Division of Elections Web site. [...] More use of internet voting would make fear of “rigging” even more of an issue than it has already become during the current election, Epstein says. If an election’s results are extremely unexpected or need to be audited, checking actual ballots is a lot more reliable than checking computer systems for signs of tampering. “Rigging an election electronically would be a lot more likely than someone going from precinct to precinct to tamper with votes,” Epstein says. “We do not know how to build foolproof [online] systems.”

https://www.scientificamerican.com/article/e-voting-refuses-to-die-even-though-it-s-neither-secure-nor-secret/

Internet Voting in Canada: A Cyber Security Perspective
Aleksander Essex, Department of Electrical and Computer Engineering
Western University
(2016-10-??)

Secure and verifiable Internet voting remains one of the most challenging open problems in cyber-security. Despite numerous potential social benefits, the technological risks are many, and the democratic stakes, therefore, remain high. We recommend the Special Committee on Electoral Reform (ERRE) not proceed with Internet voting in federal-level elections until (a) research and development efforts can create effective end-to-end election verification technologies, and (b) a national framework for secure Internet voting can be created establishing security standards, software testing requirements, government oversight, and legal accountability.

http://www.centreforedemocracy.com/wp-content/uploads/2016/10/Policy_Brief_Alex_Essex.pdf

-----

Security Issues with Online Voting
Dr. Dan S. Wallach (Professor, Department of Computer Science, Rice University)
(2016-10-??)

Companies that engage in electronic commerce make significant, ongoing investments in the security of their operations. Despite those investments, their losses are significant: "In 2015, the British insurance company Lloyd's estimated that cyber attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more." We can't afford fraud in elections. We can't simply write it off as a cost of doing business. Furthermore, in banking, if a fraudulent transaction occurs, perhaps because a credit card number was stolen, the victim will see it on their statement and can dispute it. In sharp contrast, if an Internet vote was flipped, current systems give the voter no evidence with which discover this. [...] Will we ever be able to vote on the Internet? Eventually, yes, but definitely not with today's computers, and not on today's Internet. This is an open research challenge which requires better security across the board, from consumer operating systems and web browsers through our networks and cloud infrastructure. Internet voting is a great aspirational goal, but it's not feasible yet to do this, particularly in light of the threats these systems will face.

http://www.centreforedemocracy.com/wp-content/uploads/2016/10/Policy_Brief_Dan_Wallach.pdf

-----

gcn.com
Online voting still faces security issues
(2015-03-25)

[...] fraudulent ballots are extremely difficult to detect because there is currently no reliable system online. Unlike paper or in-person ballots, "Internet elections are essentially impossible to audit, and there's no meaningful way to recount because there are no original indelible records of the voters' intent against which to compare the outcome," Jefferson stated. "The only vote records are on the server, and they are highly processed electronic ballot images that have been operated on by millions of lines of code on the client device, during transit through the Internet and on the server and canvass systems.”

So far, the best models for secure Internet voting are called end-to-end auditable cryptographic protocols, and they are still in the research and development phase.

https://gcn.com/Articles/2015/03/25/Internet-voting-insecure.aspx

-----

Lawrence Livermore National Laboratory
Security risks and privacy issues are too great for moving the ballot box to the Internet
(2015-03-10)

Newer Internet voting architectures are Web-based systems in which voting transactions superficially resemble ecommerce transactions. While better than email voting, Web-based systems are still riddled with intractable security problems, including client-side malware attacks, server-side penetration attacks, denial of service attacks, voter authentication attacks and network attacks of various kinds. Third-party vendors of such systems, unsurprisingly, deny or downplay any security risks to the system, he said.

He notes that online shopping requires no strong authentication or verification of eligibility, only demonstration of the ability to pay. Criminals, foreign nationals, minors, or almost anyone are free to shop online. Proxy shopping transactions on behalf of someone else are perfectly legal, Jefferson said, whereas proxy voting definitely is not. Another requirement that sets voting systems apart from online shopping and banking is the need for "a system to be transparent while still protecting the secrecy of who cast which ballot." There is no comparable requirement for e-commerce. With online shopping, errors and fraud will eventually be detected and can usually be corrected later, but because of the secret ballot requirement voting transactions must be recorded accurately the first time since vote manipulation is not generally detectable or correctable. "Also, financial losses in e-commerce can be insured or absorbed, but no such amelioration is possible in an election," he said. "And of course, the stakes are generally much higher in a public election than in an e-commerce system."

https://www.llnl.gov/news/security-risks-and-privacy-issues-are-too-great-moving-ballot-box-internet

-----

TheConversation.com
NSW’s online gamble: why internet and phone voting is too risky
(2015-03-10)

[...] polling place-based electronic voting with a voter-verifiable paper record can provide proper peace of mind for voters and political candidates alike. But as yet, no remote telephone or internet voting system in Australia or overseas truly provides reliable, usable, verifiable and private voting.

http://theconversation.com/nsws-online-gamble-why-internet-and-phone-voting-is-too-risky-37465

-----

cnet.com
Critical iVote security flaws expose risk of online voting fraud
(2015-03-23)

The researchers studied code and design documents behind iVote and built a proof of concept that demonstrated how the site's flaws "could be used by an attacker to steal votes".

"In our demonstration, the malicious network injects code that stealthily substitutes a different vote of the attacker's choosing," they wrote. "We also show how the attacker can steal the voter's secret PIN and receipt number and send them, together with the voter's secret ballot choices, to a remote monitoring server."

The security experts also wrote about issues with vote verification, saying there were a number of points of weakness in the iVote system that could be exploited by hackers. Because voters are instructed to verify their votes by a website that is itself vulnerable, they could be directed to an incorrect phone verification line, or the instructions to verify might not be displayed at all.

"An unverifiable Internet voting system may seem to be secure but actually be subject to undetectable electoral fraud," they wrote. "In a way, iVote is worse: a system that seems to be verifiable but possibly isn't."

https://www.cnet.com/au/news/critical-vulnerabilities-ivote-security-flaws-online-voting/

-----

news.com.au
Why is Australia still not voting electronically on election day yet?
(2015-10-30)

Of the countries that have moved towards online voting or computer-assisted voting, some have had problems of their own.

Security breaches or technical glitches have resulted in some e-votes being declared invalid during elections in Finland and the Netherlands, while during the US general elections in 2006, some electronically cast votes intended for Democratic candidates were actually recorded as Republican. [...]

“I think in the polling place there are quite sensible solutions, but I think over the internet it is just an unsolved problem,” Dr Teague said.

“The option for running genuinely verifiable, genuinely private and usable internet voting in the presence of the kinds of security threats that are out there on the internet are just not solved yet.

“I think whenever we’re considering what the (voting) options are, we have to think about scrutiny and verifiable evidence integrity. If we’re thinking about a particular technology — and that might be convenient, it might be appealing, it might be all kinds of things — we have to think about that option in terms of what would be the process for security and giving people verifiable evidence that we got the right answer.”

http://www.news.com.au/technology/online/security/why-is-australia-still-not-voting-electronically-on-election-day-yet/news-story/f971e7a8d2441050c5ed5e0ece8d0833

Electronic Frontier Foundation (EFF)
New South Wales Attacks Researchers Who Found Internet Voting Vulnerabilities
(2015-04-06)

Criticizing Halderman and Teague for identifying security flaws in an Internet voting system is like criticizing your friend for pointing out that the lock on your front door doesn’t work. While moving to Internet voting may sound reasonable to folks who haven't paid any attention to the rampant security problems of the Internet these days, it's just not feasible now. As Verified Voting notes: "Current systems lack auditability; there’s no way to independently confirm their correct functioning and that the outcomes accurately reflect the will of the voters while maintaining voter privacy and the secret ballot." Indeed, the researchers' discovery was not the first indication that New South Wales was not ready for an Internet voting system. Australia’s own Joint Standing Committee on Electoral Matters concluded last year, “Australia is not in a position to introduce any large-scale system of electronic voting in the near future without catastrophically compromising our electoral integrity.”

https://www.eff.org/deeplinks/2015/04/new-south-wales-attacks-researchers-who-warned-internet-voting-vulnerabilities

Charlie Cares

***

I would ask that we be vigilant and put more investigation into this issue.

Yes - it is might convenient, but we need to look very carefully at the problems that could be caused.

Karen Sweigard

***

Dear Mayor and City Councillors,

I don't support online voting in the upcoming municipal election. However, I may be supportive if the following issues are resolved at some point in the future:

- That MPAC voters list is significantly flawed leaving the list of electors questionable. Without in person elections staff it will be impossible to correct errors.

- The probability of voter fraud is significantly increased

- That the technology has not proven to be robust enough to guarantee that the results won't be manipulated

Furthermore, a system to ensure accessibility for those unable to get to polling stations can be instituted without online voting.

We are not ready for online voting - yet.

Evan Ferrari

***

I just want to write about my concerns regarding e-voting. It seems that at this time experts agree that it is not completely secure. I think we should take pause in regards to this issue and wait until such time that it is secure.

Voting is a fundamental right in Canada, and I don't want that compromised with technology that may prove unreliable.

As much as I love the convenience of e-voting, I think the possibility for tampering, or losing data far too great a risk at this time.

I'm looking forward to progress made in this technology and I'm sure e-voting will be a convenience we may all enjoy in the future, but at this time I'm sure we can find better solutions for people who may have difficult getting to the polling stations.

Sincerely,

Chantal Lapointe

***

Please keep Guelph moving forward into the future, and allow online voting.

Thank you,

Jackie Speers

***

Good morning,

This email is in support of keeping the online voting system in place. It proves effective and easily accessible for majority of your voters.

Sincerely,

Theresa Barras

***

Dear Mayor Guthrie and Councillors,

I would like to be very clear in my voice regarding the movement toward on-line voting in upcoming elections.

I was a victim of voter fraud through robo-calls.

I do not support on-line voting.

Thank you,
Kelly McCullough

***

As a resident of Guelph, I strongly support the preservation of online voting in our city.

Patrick Stevens

***

It's a must. Why is this being discussed in 2017?

Mark Kidd

***

Definitely want to add my name to those in favour of online voting in Guelph. I didn't take advantage of it last time but would in the future.

Thank you,

Kelly Caldwell

***

I am emailing this morning to express my displeasure that Guelph is considering removing accessible online voting for the 2018 election.

While I myself voted in-person, there are so many Guelph residents for whom I believe this to be an indispensable service, and the only reason that they were able to vote in 2014.

For the city to remove this would be akin to disenfranchising them.

Thank you!

Andy Saunders

***

I feel accessible, online voting should be saved!!

Lynda Murray

***

Hello,

I would like to voice my opposition to electronic voting. Our current system is secure and the public can trust its security. The same cannot be said for electronic voting.

Thank you, Nigel Brown

***

Please continue online voting for the 2018 municipal election in Guelph.

Thank you,

Kevin Librach

***

Dear Sir/Madam:

I would like the city to know that I believe accessible online voting is a forward thinking method that works well and should be a part of our crucial voting system.

Best regards,

Tammy LaPierre Thompson

***

Please Keep Online Voting.

Thank you

Carlie Roberts

***

Dear madam/sir:
I would like to request you to save online voting.
Thank you.
Kiran Raj Pandey

***

Hi,

Though I personally did not use this service when go big in the last local election I truly feel this is an valued option that needs to be available for those that do not have access to polls. As Guelph General Hospital has now introduced free and secure wifi to patients and visitors, think of all the hospitalized patients who could access this service.

If 13,000 people accessed this service in the previous election that should prove it's value.

Please keep email voting an option for upcoming elections,

Amy Wright

***

Good morning,
I would like to say I'd love for online voting to be an option! Thank you!
Thanks and have a lovely day!

MICHELLE WOOD

***

Online voting is necessary to be kept available for all future elections please!
Amanda van de Pol

***

I feel online voting should be kept. More voter turn out means a better voice heard from the people. Please allow online voting to continue.... or release proof that fraud actually occurred.

Matt Peters

***

Hello,

Please don't put an end to online voting. Think of the people who can't get out of their homes because of disabilities, you're taking away their voices.

Jason Inglis.

***

Although I think on-line voting potentially has many advantages, I would like to express my support for those who think we should NOT use this method of voting until we can be fully confident in its security and the accuracy of the voter's list supplied by MPAC.
Susan Merritt

***

I think online voting should be allowed in upcoming election.
Rob Green

***

Hello,

Online voting should be saved and used for the 2018 elections

Thanks!
Kate Marentette

***

Yes for Accesible online voting
Ataharul Chowdhury

***

Hello,
I just want to write my support for accessible online voting. I have lived in Guelph my whole life, and as a disabled member of the community, I think that online voting is incredibly important in order to make sure everyone has a fair chance to be heard in their city. When I was 25, I had a massive ischemic stroke that left me paralyzed in one leg and also caused chronic pain and fatigue. I have no license, and getting to the bus stop is tiring and painful and difficult. I can book a mobility bus, but they are almost always overbooked on a regular day. I can't imagine I would be able to schedule a spot for election day when I can't even get a ride to the dentist on a random Thursday afternoon, booking days in advance.

So for someone like me, who cares about the community and deserves to have a say in the way my government is run, please keep online accessible voting. It doesn't make sense to stop progression simply because something may or may not happen in the future. Elderly and disabled people deserve the same ease of access to voting as everyone else, and in my opinion that would not be the case if online voting is denied in 2018. If problems arise in the future, I think we should address them, but there is no point in silencing a large portion of the voting population over a "what if". That's undemocratic. There are many precautions that I'm sure will be taken to ensure voter security, and if those precautions are not enough then we should deal with it when problems arise. Please don't silence people like me.

I have a lot more to say, but I didnt realize the deadline was this morning and I have to go. Thank you for your time and consideration. Please take disabled and elderly people into consideration as you move forward to finding a solution to this issue. It's hard enough to get around Guelph as it is with a disability (this is honestly an area I feel that Guelph has massively dropped the ball) so please keep that in mind during your deliberations. I want the opportunity to be involved in my local politics! I want to be able to be engaged with the ease of access that many other people have already.

Thank you,

Laura Root

***

I believe online voting should be allowed in the next election.

Thank you.

Lana Haines

***

The 0nline voting option should be preserved.

Dennis Gray

***

Mayor Guthrie, Councillors –

At first blush, online voting is seductive and compelling. I, along with many fellow citizens, was sold on the idea.

However, having listened to others and read the persuasive anti-letters to the *Tribune* editor, I’m no longer convinced.

If voting were secure, I would still be in favour, but according to many in-the-know, it isn't.

Until such time as it is, I urge Council to stick with the tried and true method of being vetted at the polling station and dropping one's vote into the ballot box.

Besides, voting is a social activity ... There is pleasure to be had in visibly exercising one's democratic right along with one's fellow citizens.

Of course, every effort should be made to transport / accommodate people who have difficulty getting to or into their polling station. Any expense incurred will likely be less than that incurred by establishing online voting.

I must add that I am disappointed that the mayor has waged a not-so-subtle campaign against councillors whose opinion differs from his.

There is something undemocratic, dare I say Trumpian, in the tactic he has adopted. I expect more from a civic leader.

John Parkyn

***

Please ensure we are counted in for keeping the electronic vote.
Vincent and Kimberley Rogers

***

Dear Mayor and Councillors,

I am concerned that the city is spending money on e-voting, despite the fact that it has not been shown to always increase voter turn-out.

Proving that an increase in voter turn-out is due to e-voting alone is very difficult, because so many other factors contribute to voter turn-out.

I am very concerned about security issuesand that the e-voting system is vulnerable to hacking and fraud.

I urge council to vote against e-voting.

Thank you,

Julie Horrocks

***

If there are security concerns with online voting, address them. But scrapping online voting will make it impossible for some to actually cast a vote. Not everybody is able to show up in person to the polling station. Democracy is for everybody.

Dave Kaczorowski

***

April 18, 2017

Mayor Guthrie and members of Guelph City Council,

Re: Lack of security for Internet Voting

Sent by email. (This letter was included in your package but without my name as per City policy. I am re-sending this message with my name included see Note below)

By way of explanation, In 2011, I was a victim of the Sona robo-call fraud. My privacy and my right to vote are very important to me and this incident shook me to the core. I registered a complaint with the government. In the following federal election, my name seemed to disappear from the voter roll. I received little satisfaction or assurances from the government that there would not be a future problem.

I sat in the courtroom at the sentencing hearing of Mr. Sona and distinctly heard the judge say that he did not believe that Mr. Sona acted alone. Yet no further prosecutions have taken place. I consider this event unresolved and the conviction of Mr. Sona has done little to reassure me.

I have spent considerable time reading about internet fraud and electronic voting fraud. My informal research has not allayed my fears and has left me with a healthy distrust of electronic voting.

There have been so many incidents of electronic hacking in the United States and around the world as well as in Canada. The number of fraudulent telephone calls and emails are growing exponentially. Software giants like Microsoft and Facebook release security updates on a continuous basis. My son's Sony account was recently was hacked as well. How can the city possibly afford this service to secure on-line voting?

For these reasons, unless the City can provide me with **absolute** assurances that my privacy will be maintained and that my vote will be secure, I **do not** support internet voting at this time.

Yours, truly,

Margaret Carter

***

Hello,

Please acknowledge my opposition to electronic voting. As someone who received a robocall two elections ago, and witnessed the subsequent inability to discern where things went wrong, I am shocked that anyone would consider electronic voting to be secure. I do not support this insane notion.

Norman Liota

***

Internet Voting in Canada: A Cyber Security Perspective

Aleksander Essex
Department of Electrical and Computer Engineering
Western University, Canada
aessex@uwo.ca

Summary. Secure and verifiable Internet voting remains one of the most challenging open problems in cyber-security. Despite numerous potential social benefits, the technological risks are many, and the democratic stakes, therefore, remain high. We recommend the Special Committee on Electoral Reform (ERRE) not proceed with Internet voting in federal-level elections until (a) research and development efforts can create effective end-to-end election verification technologies, and (b) a national framework for secure Internet voting can be created establishing security standards, software testing requirements, government oversight, and legal accountability.

I. Introduction

You can bank online. You can shop online. You can file your taxes online. You can renew your license online. Why don't you vote online? It seems like a natural use of the technology. The perceived advantages of Internet voting typically center on otherwise reasonable goals like increasing voter turnout, reaching under-represented populations, improving accessibility and decreasing election costs. But one of the main reasons we don't vote online already is because, simply put, Internet voting is a really difficult security challenge that we haven't solved.

As a simplification of a very complex problem, the reason Internet voting is harder than other cyber-security systems comes down to the a fundamental tension between the security goals of ballot secrecy, and election integrity. If we simply did away with the secret ballot, Internet voting security would become much more tractable, and resemble other security systems, like online banking.

The technical challenge of electronic voting comes from requiring security and secrecy at the same time. How do you prove my vote counted, when you don't know what my vote even was? This can be accomplished in a suitably reliable fashion with paper ballots and in-person polling through a combination of physical and procedural security measures, along with the immediately observable nature of the physical word. There is, however, no direct software analogue to the physical guarantee that paper ballots going into an empty box are the same as what comes out at the end of the day.

II. Threat Overview

In its most basic form, contemporary commercial Internet voting systems consist of a standard web-application framework; a voting program (typically Javascript) is sent from the election server across the Internet to your browser. When you cast a ballot, the information about your selections is returned to the server and stored in a database to be tabulated later. Security is required at all points in this chain: at your device, in transit, and at the election server.

From a security perspective, this architecture introduces a host of potential threats not found in Canada's current in-person hand-counted paper ballot method.

Vote Selling and Coercion. Because of the inherent unsupervised nature of Internet voting, individuals can be observed by others while voting, and thus could be unduly influenced in their voting intentions.

Phishing. Numerous online avenues exist to misdirect voters into visiting misleading or malicious websites, or visiting legitimate URLs that deliver, for example, cross-site scripting payloads.

Automation bias. Habituation and lack of comprehension about the goals and purpose of common web security technologies can lead users to place an undue reliance on technological protections, as well as underestimate the significance of warnings or errors. Examples include not noticing when the green padlock icon is missing, or clicking through browser security warnings. This is further complicated by the fact that many websites (see e.g., https://elections.on.ca) generate errors due to simple misconfigurations.

Denial of Service. The distributed nature of the Internet makes it possible for a server to be flooded with connection requests from numerous distributed machines. Although technological mitigations exist for attacks of this kind, they do occasionally cause significant disruptions. For example, a denial of service attack in 2015 caused Canadian federal government websites to be inaccessible for several hours.

Client-side Malware/Spyware. Owing to our connected lifestyle, the computational device we would use to cast a ballot would likely have previously been used in many other contexts. Numerous opportunities thus exist to inject malicious software onto a voter's computer with the intention of altering and/or surveilling ballot selections. Any acceptable Internet voting system must be robust, even in the presence of malware.

Network attacks. Numerous possibilities exist for an internet attacker located in between the network connection of a voter and the election server to attempt to view or modify ballot data. A fundamental and necessary security protection is Transport Layer Security (TLS), which is commonly denoted in your browser as a green padlock. User errors, server-side misconfigurations, and novel cryptographic attacks can all be leveraged in a "man-in-the-middle" attack to access or alter voter preferences. Despite this being a core internet security technology, we found that of the 14 federal, provincial, and territorial election agency websites, only Elections Nova Scotia supported TLS. Further, we found TLS misconfigurations in the Elections Ontario and Elections PEI websites. See Table 1.

Agency	TLS Support	Server Location[1]
Elections Canada	Unsupported	Canada
Elections Alberta	Unsupported	U.S.
Elections BC	Unsupported	Canada
Elections Manitoba	Unsupported	Canada
Elections New Brunswick	Unsupported	Canada
Elections Newfoundland	Unsupported	Canada
Elections NWT	Unsupported	Canada
Elections Nova Scotia	Supported	Canada
Elections Nunavut	Unsupported	Unknown
Elections Ontario	Misconfigured	U.S.
Elections PEI	Misconfigured	Canada
Elections Quebec	Unsupported	Canada
Elections Saskatchewan	Unsupported	U.S.
Elections Yukon	Unsupported	Canada

Table 1. Current TLS Support Across Canadian Election Agency Websites

Server penetrations. A Canadian federal election today technically consists of 338 separate elections held in thousands of separate polling places spread across the country. An Internet-based system consolidates all of these on to one internet-facing server, reachable by any computer in the world. Any combination of undisclosed software vulnerabilities, misconfigurations, or human error could allow a remote attacker to gain access to voter registration information or ballot data. Instances of server penetrations (e.g., ransomware, email and password dumps, IP theft, etc.) are becoming increasingly common, and examples can be found across all organizational sectors.

Insider Influence. There is a risk of insiders (e.g., election officials, vendors, technicians, etc.) viewing or modifying ballot selections on the

[1] Based on iplocation.net consensus.

server, making it vital for there to be strong mechanisms to prevent undetected changes to votes.

State-level Actors. Perhaps the greatest threat to an Internet election is a sophisticated attack by a state-level actor who undetectably changes an election result. Examples of such potential state-level intervention in elections have surfaced in the United States in the context of voter registry data. In a worst-case scenario the ensuing political turmoil of a stolen election could precipitate an economic collapse, or worse, a war. Further, it is not certain whether a sophisticated attack would ever even be detected. From that perspective, any federal-level Internet voting system is a critical infrastructure, and its safeguard could reasonably be viewed as a matter of national security.

III. RECOMMENDATIONS.

A. *End-to-end Verifiability.*

Recent research into Internet voting implementations has shown weak procedural security (Springall et al., 2014; Wolchok et al., 2010), and weak, vulnerable, or ad-hoc security implementations and configurations (Wolchok et al., 2012; Clark & Essex, 2014; Teague & Halderman, 2015). One promising approach is cryptographic end-to-end verifiable Internet voting (E2E-VIV), which allows voters to create privacy-preserving receipts of their ballot, which can later be used as part of a public, universally-verifiable cryptographic proof of correctness. Two notable projects include Helios (Adida, 2008) and Scantegrity/Remotegrity (Carback et al., 2010; Zagorski et. al, 2013), the latter of which was deployed in the first governmental E2E verifiable election in the city of Takoma Park, MD in 2009 and 2011.

A recent report by the U.S. Vote Foundation (Dzieduszycka-Suinat et al., 2015) has gone as far as to suggest *all* Internet elections be E2E-VIV. Owing to its extensive use of cryptography, however, many research challenges remain to make such schemes practical in terms of functional requirements (i.e., usability, accessibility, etc.) and conceptual requirements (understandability, verifiability, etc.). Giving these risks and potential avenues for developing mitigations, we recommend, therefore, ERRE *not* proceed with Internet voting at this time, and instead prioritize research into Internet voting verification technologies, and promote interdisciplinary opportunities for research collaborations to explore issues at the intersection of elections and cyber-security.

B. *National Framework for Internet Voting*

Before Canada can proceeded with Internet voting, it would be vital to establish a national framework to lay out security standards, software requirements, testing methodologies, government oversight, and legal accountability.

Regarding testing and government oversight, an advisory panel to the state of Utah (Cox et al., 2015) recently recommended that any candidate system be made available in an open trail in which the public is invited to conduct penetration testing through a series of mock elections over the Internet. As demonstrated by Wolchok et al. (2012), this can be an effective means of discovering critical vulnerabilities in a realistic, but non-live election scenario.

Regarding standards and requirements, the government does not necessarily have the in-house expertise to adequately evaluate and verify Internet voting systems. Similar to the recommendations of the Internet voting advisory panel to the Legislative Assembly of British Columbia (Independent Panel, 2014), we recommend the formation of an independent technical committee consisting of election administrators and Internet voting security experts. This committee would be responsible for rigorously evaluating the security of candidate systems.

Conclusion. ERRE should be aware that considerable concern about the safety of Internet voting exists among international technology and cyber-security experts. Echoing a statement by prominent U.S. computer technologists (Computer Technologists), we urge Internet voting only be adopted after the numerous technical threats outlined above can be suitably mitigated, and strong mechanisms put in place to prevent undetected changes. The entire system must be reliable and verifiable in a way that is convincing to the voting public.

References

[1] B. Adida. Helios: web-based open-audit voting. In USENIX Security Symposium, pages 335–348, 2008.

[2] R. T. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora. Scantegrity II election at Takoma Park. In USENIX Security Symposium, 2010.

[3] J. Clark and A. Essex. Security Assessment of Vendor Proposals, Final Report. City of Toronto RFP #3405-13-3197, 2014. https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf

[4] Computer Technologists Statement on Internet Voting. https://www.verifiedvoting.org/projects/internet-voting-statement/

[5] S. J. Cox, A. Lawrence, C. Bramble, R. Chavez-Houck, R. Cowley and others. iVote Advisory Committee Final Report for the State Utah, 2015. https://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf

[6] 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. https://www.usvotefoundation.org/E2E-VIV, 2015.

[7] Independent Panel on Internet Voting. Recommendations Report to the Legislative Assembly of British Columbia, 2014. https://www.verifiedvoting.org/wp-content/uploads/2014/10/CA-BC-2014-recommendations-final-report.pdf

[8] 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 21st ACM Conference on Computer and Communications Security. ACM, Nov. 2014.

[9] V. Teague and J. A. Halderman. The new south wales ivote system: Security failures and verification flaws in a live online election. In VoteID, 2015.

[10] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. Security analysis of india's electronic voting machines. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), 2010.

[11] 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.

[12] F. Zagorski, R. T. Carback, D. Chaum, J. Clark, A. Essex, and P. L. Vora. Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. 2

Cameron Shelley
12 Clarke St. W.
Guelph, ON
N1H 1S9

April 11, 2017

To Whom It May Concern:

Rather than simply cite numerous Canadian reports discussing why e-voting is not recommended at this time (as in my previous letter), I thought it would be more helpful to discuss these issues with specific reference to the e-voting system proposed for use in Guelph. Also, proponents of e-voting often argue that nothing has gone wrong with e-voting yet. This claim is simply untrue. To help correct this misperception, I will frame this discussion using actual examples of things that have gone wrong with e-voting.

I will use the report of the *Independent Panel on Internet Voting* (British Columbia 2014) as my main reference. Several high-level studies of e-voting in Canada have been done, all of which recommend against its adoption (see Appendix). However, the BC Report is the most appropriate for the present purpose because it is thorough, succinct, and balanced. It also drew on experience with e-voting at all levels of government, so that its conclusions are applicable to local as well as provincial and federal elections.

In the end, I hope you will agree that, in spite of the advantages of improved convenience and accessibility, the e-voting system now proposed for Guelph should not be adopted.

British Columbia (2014). *Recommendations report to the Legislative Assembly of British Columbia—February 2014*, Independent Panel on Internet Voting British Columbia. URL: http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

Convenience and accessibility

There is little question that e-voting would be superior to paper ballots in terms of convenience. Provided voters have reliable Internet access, the time and effort needed to vote would probably be significantly less than with any other voting method. As Jordan Brown of Prince Edward Island's Special Committee on Democratic Renewal put it, "You could literally sit home in your underwear at 2 a.m. and cast your ballot then as you were looking through the different options" (Pitt 2016). Who has not dreamed of voting without their pants on?

Were convenience the only consideration regarding e-voting in Guelph, it would be considered a slam-dunk.

E-voting could also make voting considerably easier disabled or overseas voters for whom travel to polling stations is problematic. Voters with visual impairments who find regular ballots difficult to read could also benefit, provided that the e-voting software is compatible with the software they use to support their document reading.

Equitable access is an important consideration. It should be seriously considered for voters for whom polling stations are simply unsuitable. There are other options to be considered for this purpose. The Town of Minto, Township of Guelph/Eramosa, the Town of Erin, and the Township of Centre Wellington used main-in ballots in their municipal elections of 2014.

Although mail-in ballots have their own shortcomings (see below), they are relatively simple, low-cost, and effective.

Pitt, S. (2014). “You could literally sit home in your underwear at 2 a.m. and cast your ballot,” CBC News. URL: http://www.cbc.ca/news/canada/prince-edward-island/pei-evoting-internet-voting-plebiscite-electoral-reform-1.3810250

Voter turnout

Increasing voter turnout is the most common argument given in favour of e-voting. The great convenience it provides would allow people to vote who otherwise would lack the opportunity. Thus, voter turnout, a perennial problem, would increase.

Although this argument is plausible, increases in voter turnout do not reliably follow from the introduction of e-voting. When other factors that influence voter turnout are considered, e-voting has not reliably proven to make any difference. The BC Report (British Columbia 2014, § 4.2) makes the following observation:

> While there have been some Internet voting elections where voter turnout has increased, when other factors such as the apparent closeness of the race and interest in particular contests (e.g., a mayoral election without an incumbent) are taken into consideration, research suggests that Internet voting does not generally cause non-voters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have already decided to vote.

This observation explains why turnout can be good after the introduction of e-voting in some cases but not others. So, Guelph saw a voter turnout of 45% in 2014, an increase of 11%, with the introduction of e-voting (Guelph 2014). However, Prince Edward Island saw an abysmal 36.4% turnout during a plebiscite on electoral reform in 2016, in spite of having introduced e-voting, vote by telephone, and extended the franchise to 16- and 17-year olds (Sinclair 2016):

> "Notwithstanding unprecedented measures taken to encourage voter turnout and to facilitate voting, just under 36.5 per cent of registered voters cast a ballot during the ten-day plebiscite voting period," said [Premier Wade] MacLauchlan in a statement.

The current, paper-ballot system provides many opportunities to vote. Decreases in voter turnout are likely due to other causes.

This point also undermines the claim made by Councilor Dan Gibson that not adopting e-voting amounts to voter suppression (Gibson 2017). I take *voter suppression* to mean an attempt to decrease voter turnout through manipulation of the election system. Since adoption of e-voting does not reliably increase voter turnout, as the reports above conclude, then non-adoption of e-voting cannot be considered an act of voter suppression.

Thus, the goal of increasing voter turnout is not a reason to adopt e-voting.

Gibson, D. (2017, April 5). “Is casting your ballot online in the 2018 Guelph Municipal Election important to you?”. Ward 1 blog. URL: http://www.ward1guelph.ca/2017/04/is-casting-your-ballot-online-in-the-2018-guelph-municipal-election-important-to-you/

Guelph (2014, Oct. 28). “Guelph 2014 municipal election results are in,” City of Guelph. URL: http://guelph.ca/2014/10/guelph-2014-municipal-election-results/

Sinclair, J. (2016, Nov. 8). “Premier calls plebiscite results 'debatable,' cites low turnout,” CBC News. URL: http://www.cbc.ca/news/canada/prince-edward-island/pei-premier-plebiscite-results-1.3842107

Vote buying and selling

Vote buying and selling refers to exchanges of votes for payment or other considerations. The practice was routine in Canada during the Victorian era. For example, candidates would serve food and liquor to voters who then voted for them at the polls. Since voters cast their votes by announcing them out loud to a record keeper in a public place, buyers could be sure that the transaction was completed as agreed. The practice of secret balloting was introduced to undermine buying and selling since voters could simply take bribes and then not follow through.

Regrettably, various forms of vote buying remain a problem, as in Montreal (Gyulai 2013):

> The phenomenon of voting illegally by impersonating a registered elector who is dead, has moved away or is simply not voting is called "telegraphing" in the Quebec lexicon. The term conjures the Maurice Duplessis era 60 years ago, when it is well known that pork barrelling, vote buying and ballot box stuffing prevailed.

The article notes that "telegraphing" remains a routine part of local politics in that city.

Perhaps the most common form of vote buying and selling occurs with mail-in or absentee ballots. Consider the following example (Derfner 2000):

> … James Baumgartner, a graduate student at Rensselaer Polytechnic Institute, had launched Vote-auction.com, an Internet marketplace for the wholesale purchase of votes. The model was simple: Recruit willing voters, auction them off in state blocs, double-check their absentee ballots for accuracy, and split the proceeds evenly. The schemes generated a lot of media attention and some sellers and buyers—the bidding on eBay reached $10,100, and Vote-auction found 200 takers in a single day.

Kind of like an Uber for vote buying and selling! Of course, the scheme was illegal and was shut down after a warning from the New York State Board of Elections. Had the site been housed outside of the United States, closing it down would have been problematic.

The absentee ballots mentioned above are ballots that voters request from their governments to be delivered to their homes. These ballots may then be filled out and then returned by mail. Since these ballots need not completed in privacy, they may be bought and sold. For example, a voter can simply sign a blank ballot and give it to a third party in exchange for money. This arrangement was the one being brokered by Vote-Auction.com.

This example is relevant because e-voting also facilitates vote buying and selling. Like mail-in ballots, e-votes are not conducted in private. In the system proposed for adoption in Guelph, anyone with a legitimate voter ID, PIN code and birthdate can log in and cast a vote (Watson 2017). So, anyone with such an e-voting credential who does not care to vote may sell that information to someone who does. In effect, the purchaser has bought the identity of the voter for the purposes of casting a vote.

This problem arose in the 2016 plebiscite in Prince Edward Island. As there was no door-to-door enumeration, an unknown number of voter ID cards were sent to the wrong addresses (Campbell 2016). Probably as a result, there were two reports of "voter error" (voters casting the ballots of others by mistake) and one report of voter fraud (a voter casting the ballot of another on purpose) which was reported to the RCMP (Campbell 2016a).

These results are certainly unwelcome in their own right. They also show that the conditions required for vote buying and selling are created in this e-voting scheme. As the example of Vote-Auction.com shows, the same technology that makes e-voting so convenient also promises to make fraudulent activity easier also.

This point is especially relevant to the Guelph situation since the PEI e-voting system was essentially the same as that proposed for use here. Also, the Guelph Voters List also contains many inaccuracies, meaning that e-voting credentials will be sent to many ineligible voters (Watson 2017). In addition, note that Guelph elections typically involve low turnouts. Thus, many eligible voters will receive legitimate credentials that they might prefer to sell rather than exercise.

Although I have found no research on selling of mail-in ballots in Canada, US experience suggests that it is a growing problem, and much more prevalent that in-person fraud (Liptak 2012). For example, mayoral elections in Illinois and Indiana have been invalidated due to fraudulent mail-in ballots. Given a ready supply of easily abused and transferred, illegitimate or unwanted e-voting credentials, it is possible that disgruntled citizens, hyper-partisans, or trolls might engage in buying and selling.

Despite risks of vote buying and selling, mail-in ballots have been used in many jurisdictions because the service is extended to only a small fraction of the electorate, e.g., disabled and overseas voters (British Columbia 2014, §5.5). The City of Guelph is proposing to extend e-voting to the entire electorate, thus undermining this rationale here.

The e-voting system proposed for Guelph also does not include measures that might mitigate this problem. For example, the Norwegian e-voting system was configured to allow voters to vote multiple times, with only the final vote counting. In that way, anyone purchasing voting credentials could not be sure that the vote they made with the bought credential would not be overridden by the original voter. (Let me observe that Norway terminated its e-voting program in 2014, nonetheless.)

A Google search of Guelph.ca for "internet voting" and "buying or selling" shows that this issue has been mentioned in connection with Guelph's e-voting scheme (Guelph 2013). However, it is not evident that it was well explained or explicitly considered by the Council.

The Council should at least discuss its rationale for increasing the risk of vote buying and selling, or simple fraud, by extended e-voting to the general electorate. They should also consider why measures that might be taken to mitigate the problem have not been adopted. This matter is a most serious one, as doubts about fraudulent votes would call the legitimacy of the Council into question.

Campbell, K. (2016, Oct. 31). "'Not a fool-proof system,' Elections P.E.I. says of online vote," CBC News. URL: http://www.cbc.ca/news/canada/prince-edward-island/plebiscite-online-voter-fraud-1.3829909

Campbell, K. (2016, Nov. 8). "Elections P.E.I. not ready to recommend online voting in next election," CBC News. URL: http://www.cbc.ca/news/canada/prince-edward-island/pei-plebiscite-online-voting-1.3841893

Derfner, J. (2000, Aug. 23). "Buy this vote!" Slate.com. URL: http://www.slate.com/articles/news_and_politics/net_election/2000/08/buy_this_vote.html

Guelph (2013, July 29). "City Council agenda." URL: http://guelph.ca/wp-content/uploads/council_agenda_072913.pdf

Gyulai, Linda (2013, Aug. 15). "Fraudulent voting often the way elections are won." Montreal Gazette. URL: http://www.montrealgazette.com/news/Fraudulent+voting+often+elections/8694078/story.html

Liptak, A. (2012, Oct. 6). “Error and fraud at issue as absentee voting rises,” New York Times. URL: http://www.nytimes.com/2012/10/07/us/politics/as-more-vote-by-mail-faulty-ballots-could-impact-elections.html

Watson, S. (2017, Apr. 13). “Guelph Council is right to be wary about online voting,” Guelph Mercury-Tribune. URL: https://www.guelphmercury.com/opinion-story/7242775-guelph-council-is-right-to-be-wary-about-online-voting/

Control

One of the dangers that the City of Guelph risks in outsourcing its elections is that of compromising control over its electoral process.

Consider the experience of electronic voting in the Netherlands (Oostveen 2010). Electronic voting machines were first adopted there in the late 1980s and had become widespread in elections at all levels by the mid 1990s. By 2006, 90% of all votes in the country were cast using the Dutch-built Nedap/Groenendaal ES3B voting computer system. After 2004, citizens living abroad were permitted to cast votes on the system via the Internet.

In 2006–07, a grassroots campaign entitled *Wij vertrouwen stemcomputers niet* (“We do not trust voting computers”) demonstrated that the system was seriously flawed and easily hacked and manipulated. Through Freedom of Information Act requests, it also discovered that Dutch governments had lost control of their electoral process to the companies that provided their voting systems.

For one thing, Dutch governments had not acquired and maintained adequate resources or expertise to oversee their voting system. As a result, Dutch regulations were inadequate and voting machines that passed their technical requirements remained significantly insecure. Furthermore, because voting machine certification was undertaken by a firm contracted to Nedap, detailed test results were considered proprietary information and not reported to the governments. Indeed, because they were proprietary, the company maintained that governments, and thus the public, had no right to the test results.

Having adopted a completely passive role in their own elections, Dutch governments and people had little idea of how they actually worked.

In 2005, it became unclear whether or not Groenendaal, which supplied the system software, would continue operations. Realizing that they might be left with a system they likely could not operate or maintain, the Dutch Electoral Council advised the government to reconsider its relationship with the company. Feeling its business interests in jeopardy, the company replied by blackmailing the government, threatening to cease “cooperation” if the government did not agree to its demands. For example, it demanded that a computer expert and member of *Wij vertrouwen stemcomputers niet* be kept off of a commission that the government proposed to set up to review its electoral arrangements, obviously fearing a negative assessment. It also suggested a quid pro quo: “The Ministry buys the shares of our company at a reasonable price, … and we will still cooperate during the next election,” that is, the upcoming provincial elections (Oostveen 2010, p. 214). Shortly before those elections, apparently unsatisfied with the government’s response, the company head emailed the Electoral Council saying, “I have ordered my employees to halt all activity until we have received an answer that is acceptable to us.”

The Dutch government struck two commissions of inquiry into its voting system. The commission tasked with reforming the election system examined the alternatives and identified paper balloting as the preferred option. In 2008, the Dutch Parliament instituted a national moratorium on the use of electronic voting machines and (re-)adopted paper-and-pencil balloting (Goldsmith & Ruthrauff 2013).

Due to its lack of resources and expertise, coupled with a complacency engendered by the appearance that all was well, Dutch governments ceded control over their elections to the private sector. As a result, more and more decisions about the conduct of Dutch elections were made by the vendors instead of the governments.

When governments outsource their elections to e-voting firms, they tend to view it as a simple transaction: They set out some rules and make a payment, and the vendor provides the online election. On the contrary, they are making a substantial commitment. The commercial interests of private providers are not always consistent with the public interest that governments should represent. If governments do not maintain and exercise the resources and expertise needed to oversee private providers, then they may well end up with an electoral system they no longer comprehend or control, as happened in the Netherlands. Municipal governments, like the city of Guelph, are in the least advantageous positions in this respect: They often lack resources and expertise in the first place and would have difficulty in make the expenditures necessary to develop and maintain them.

Goldsmith, B and H. Ruthrauff (2013). "Implementing and overseeing electronic voting and counting technologies: Case study report on electronic voting in the Netherlands," United States Agency for International Development (USAID) under award No. DFD-A-00-08-00350-00. URL: https://www.ndi.org/sites/default/files/5_Netherlands.pdf

Oostveen, Anne-Marie (2010). "Outsourcing democracy: Losing control of e-voting in the Netherlands," *Policy & Internet 2*(4): 201–220. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.296.7735&rep=rep1&type=pdf

Transparency

The Dutch example illustrates the importance of transparency in the adoption of e-voting. Transparency is fairly straightforward in a paper ballot system. For example, a candidate who wants to ensure that ballot counting is being done properly can simply watch the process and object if it seems to be conducted improperly.

When a computerized vote counting system is used, this sort of transparency disappears. Consider the following example (Corrigan 2008, p. 148):

> There was a wonderful illustration of the difficulty in monitoring electronic elections in the 2002 Governorship election in Nebraska. The law in Nebraska states that the candidates are entitled to watch the count when the votes have been cast. One of the candidates, eager to see democracy in action asked if he could be allowed to monitor the count. He was shown an optical scanning machine and then a computer in another room with a blank screen.

The Ontario Municipal Elections Act (Ontario 1996) contains similar provisions:

> …
>
> **Scrutineers at election of candidate**
>
> 16. (1) A candidate may appoint scrutineers to represent him or her during voting and at the counting of votes, including a recount.
>
> …
>
> **Objections**

> [54. (1)] (3) A scrutineer or certified candidate may object to a ballot, or to the counting of some or all votes in a ballot, on the ground that the ballot or votes do not comply with the prescribed rules.

If the City of Guelph adopts the e-voting system proposed, then it will be in a similar situation to the State of Nebraska in 2002. If a candidate or scrutineer demands to exercise their right to scrutinize the counting process, it is not clear that the clerk would have any meaningful response available. In fact, in our era of cloud computing, the computers performing vote counting may be far away from the site of the election.

In place of transparency, governments often settle for audits of e-voting systems. For example, a third party could be hired to assess an e-voting system. This approach was the one taken by the Dutch government. This example reveals a common weakness of the approach. Because their software is proprietary, e-voting providers normally require non-disclosure agreements. That is, auditors can look at the software but cannot talk about it in any detail with third parties. So, audits do not really provide transparency in the traditional sense.

As pointed out in BC report (British Columbia 2014, §5.6), audits are generally rare and limited in scope in any event. Due to the expense involved, municipal governments are least likely to require meaningful audits. A Google search of Guelph.ca for terms "internet voting" and "audit" does not reveal any plans for the city to conduct such audits. The term "audit" *is* used to describe the process of calibration (Guelph 2014a), that is, testing of e-voting equipment to see that it is ready for use. Obviously, this form of auditing contributes nothing to transparency either.

This point reinforces the one made regarding control above. When governments outsource elections as Guelph proposes to do, they lose knowledge of how their elections actually work. At a minimum, a thorough auditing regime should be prepared before e-voting is used. Preferably, the City should only institute electoral systems that it adequately understands and controls.

Corrigan, Ray (2008). "Technology is just a tool," *Digital decision making: Back to the future*, ch. 7, Berlin: Springer Verlag.

Guelph (2014a). "Procedures for voting and vote counting equipment for the 2014 municipal election." URL: http://vote.guelph.ca/wp-content/uploads/Procedures-for-Voting-and-Vote-Counting-Equipment.pdf

Ontario (1996). "Municipal Elections Act, 1996, S.O. 1996, c. 32, Sched." URL: https://www.ontario.ca/laws/statute/96m32

Security

Security risks that affect any e-voting scheme are legion and so I refer to the overview provided in the BC report (British Columbia 2014, §5.1). However, security concerns are sometimes dismissed as mere "what-ifs" by supporters of e-voting. Here, I will briefly describe some actual instances of security problems with e-voting and the implications they have for Guelph.

For example, in October 2010, the Washington D.C. Board of Elections and Ethics took the unusual step of inviting all comers to try to hack into their e-voting system during a special week-long test period. (I say this step is unusual since, as illustrated by the Dutch example, e-voting providers and clients seldom risk receiving bad news.) Within 36 hours, Professor J. Alex Halderman and some of his students at the University of Michigan Center for Computer Security and Society had gained control of the system over the Internet. As proof, they reprogrammed it as follows (Moore 2010):

> The researchers rigged the system to play [the Michigan fight song] "The Victors" after each new ballot was cast. And they changed all the votes to write-ins for famous robots and computers such as Johnny 5 (from the movie "Short Circuit"), HAL 9000 (from "2001: A Space Odyssey"), and Deep Thought (from "A Hitchhiker's Guide to the Galaxy").

The article does not state which computer won. The intrusion was not detected by the system's administrators. So, had the intruders chosen to make more subtle changes, no one would have been the wiser. As a result of this demonstration, the Board cancelled the use of e-voting for the upcoming election.

While attacks of this nature require some sophistication, other attacks require none. For example, e-voting for the leadership of the federal New Democratic Party at their national convention on March 24, 2012 was disrupted by a Distributed Denial of Service (DDoS) attack (Payton 2012). A DDoS attack involves bombarding a computer system with service requests with the goal of slowing it down or causing it to crash. Such attacks typically originate from a "botnet", that is, a large collection of Internet-connected devices that are under the control of hackers. This attack delayed voting for several hours. Scytl, the provider of the e-voting system, was unable to identify the source of the attack. As a result, the identity and motivation of the attacker remains unknown.

Note that DDoS attacks can be hired on the Internet on a turnkey basis (Francis 2017). Someone using a DDoS-for-hire service can organize an attack simply by selecting the desired severity and duration of the attack, specifying the target, and paying. All transactions are encrypted and anonymous, and prices begin at around $20 (US).

DDoS attacks can be more damaging than the one launched against the NDP system in 2012. A DDoS attack on October 20, 2016 crashed the online Education and Quality and Accountability Office literacy test prepared for Ontario Grade 10 students in 2016 (Rushowy 2016). As a result, almost 150,000 students were unable to write the test and the $250,000 exercise had to be cancelled. The source of the attack has not been identified, although there has been speculation:

> "I would not be surprised if a teenager was behind it," added [cyber security lawyer Imran] Ahmad, of Miller Thomson LLP. "The skill set among the younger generation is extremely advanced."

The test was finally administered on March 30, 2017—on paper.

One common countermeasure against DDoS attacks is to set the deadline for online voting a few days in advance of the deadline for voting at the polls. So, if an attack occurs, then the Clerk can extend the online deadline so that, hopefully, those who were unable to vote online may do so. However, this measure raises further issues. Voters who were prevented from voting due to the attack may not get the news in time. Furthermore, they may not be able to access the system in time due to other commitments.

Voters who do access the system during an attack will be in an even more problematic situation. They will likely experience delays, dropped connections, and odd behaviour from the system. Various errors may occur, such as the system registering a vote incorrectly, or registering an under-vote (e.g., no vote) or an over-vote (e.g., voting for more than one candidate for mayor). Of course, the system has some features intended to prevent these mistakes but systems often do not work as intended while under attack. Voters in this situation will have justified doubts that their votes have been registered correctly.

In this situation, there is nothing the City can do to provide reassurance. Its proposed e-voting system does not allow online voters to look up how their vote was registered. Neither does the City's e-voting system allow e-voters to replace their online votes with paper ballots at the polls. The e-voting system in Estonia observes the principle of the "supremacy of the paper ballot", meaning that e-voters can override their e-votes with a paper ballot at the polls. One of the virtues of this arrangement is that e-voters who are unsure about how their votes were registered electronically can be sure that their votes are registered as intended.

Guelph e-voters have no such opportunity or assurance. It would not surprise me, however, if Guelphites who have doubts about their e-votes simply show up at regular polling stations looking to finalize their selections. This situation will be awkward, at best.

To avoid this issue, the City could require e-voters to waive their rights to private or accurate ballots. For example, the State of Alaska uses an e-voting system that requires users to agree to these terms before casting their votes (Hsu 2014):

> When returning the ballot through the secure online voting solution, you are voluntarily waiving your right to a secret ballot and are assuming the risk that a faulty transmission may occur.

No doubt, most users will accept these conditions without either reading them or understanding their implications. Thus, in the event of trouble, voters will likely not be understanding when the City says, "well, you knew the risk."

In Guelph, we have the case of Michael Sona and the Robocall scandal of 2011 to remind us that the use of electronic means to disrupt elections is no idle concern. In particular, when potentially effective attacks are cheap, easy, and essentially risk-free for the attacker, the temptation may prove too much for bored teenagers, hyper-partisans, disgruntled citizens, or trolls. At the same time, such an attack could easily leave the City in a position where hundreds or thousands of voters are unsure that their votes were registered properly and that the winners of the election are truly legitimate.

Francis, R. (2017, 15 March). "Hire a DDoS service to take down your enemies," CSO Online. URL: http://www.csoonline.com/article/3180246/data-protection/hire-a-ddos-service-to-take-down-your-enemies.html

Hsu, J. (2014, 6 November). "Alaska's online voting leaves cybersecurity experts worried," IEEE Spectrum. URL: http://spectrum.ieee.org/tech-talk/telecom/security/alaska-online-voting-leaves-cybersecurity-experts-worried

Moore, N.C. (2010, 7 October). "Researchers hack into DC voting system test bed, leave fight song signature," University of Michigan Engineering News Center. URL: http://www.engin.umich.edu/college/about/news/stories/2010/october/researchers-hack-into-dc-voting-system-test-bed-leave-fight-song-signature

Payton, L. (2012, 24 March). "NDP leadership vote marred by online attacks, low turnout," CBC News. URL: http://www.cbc.ca/news/politics/ndp-leadership-vote-marred-by-online-attacks-low-turnout-1.1140043

Rushowy, K. (2016, 24 October). "Cyber attack to blame for Grade 10 literacy test chaos," Toronto Star. URL: https://www.thestar.com/news/gta/2016/10/24/cyber-attack-to-blame-for-grade-10-literacy-test-chaos.html

Recounts

In the Ward 3 contest of Guelph's 2014 Municipal election, June Hofland won a place on Council over Craig Chamberlain by five votes (Guelph 2014b). Given the closeness of the result, a recount was conducted that came to exactly the same conclusoin. The process was described in the City's press release as follows (emphasis added):

> As per the Municipal Election Act, the ballots were recounted in the same manner in which they were counted on October 27. Guelph's City Clerk **re-entered the online ballots** and City staff **inserted the advanced in-person and election day ballots** into the same tabulators used at the Ward 3 voting locations.

In fact, the Clerk's use of the terms *ballot* and *recount* here is confusing in an important way. Online ballots and in-person ballots are not the same sort of thing in this case. Thus, recounts are not the same sort of thing here either. That is problematic.

To clarify, note that the term *ballot* can mean two different things. Consider the following sentences:

1. The voter put his *ballot* in the ballot box. (*ballot* = piece of paper)
2. The voter cast her *ballot* for mayor. (*ballot* = vote for a candidate)

In the first sense, a ballot is something with a list of candidates' names on it, like a piece of paper or the surface of an iPad, say, that a voter alters through interactions like making pencil marks in the former case or pushes and swipes on an iPad screen in the latter. In the second sense, a ballot is a vote that a voter means to cast for a candidate by means of these interactions.

Note that the e-voting system used in Guelph produces no ballots in the first sense. When a voter presses the surface of their iPad, say, using an e-voting app, the app interprets these actions as a vote for a candidate and then transmits this interpretation over the Internet to a computer that stores it. That interpretation—i.e., vote—is then used in counting and recounting processes.

So, when the City Clerk said that "in-person ballots" were recounted, he meant actual ballots. However, when he said that "online ballots" were recounted, he meant votes as interpreted by the e-voting system. The e-voting system contains no record of what its users were shown or did to produce the votes in question.

To see what difference this distinction makes, consider the purpose of a recount of actual ballots as understood traditionally. The point of recounts has been to ensure that the intentions of voters were honoured. Since the intentions of voters are reflected in their ballots, recounts have always required that ballots be re-examined to check that they had been interpreted properly. Running paper ballots through a voting tabulator is meant to perform such a check. In addition, everyone of sufficient age likely recalls the notorious "hanging chads" scenes during recounting of ballots in several Florida counties during the 2000 US Presidential elections. Although the process may have looked silly, re-examination of ballots has always been the method adopted in recounts to ensure that voters' intentions are correctly interpreted and respected.

Because of the lack of actual ballots, the Guelph recount of "online ballots" of 2014 was in no way an attempt to see that the will of online voters was correctly interpreted and respected. Instead, the votes as interpreted by the e-voting system were *assumed* to be correct. The test showed only that the system got the same answer both times it added up the votes in its records. In other words, the recount shows only that the e-voting system can add reliably.

While this information may be reassuring, that has never before been the purpose of recounts. The BC report (British Columbia 2014, §5.6) nicely summarizes how e-voting systems change the meaning of a recount:

> Due to the nature of how Internet ballots are cast, the concept of a recount under an Internet voting system shifts from a reconsideration of each ballot that was cast to an audit of the integrity of the system and processes by which those ballots were cast. This is a fundamental change to how stakeholders currently view the process.

Put another way, e-voting changes the meaning of a recount from a reconsideration of actual ballots to an exercise in arithmetic.

One consequence of this situation is that the outcomes of recounts of each type must be interpreted differently. In a traditional recount, if it is conducted properly, there is a chance that the total vote count for each candidate may change from the original count. This is because some ballots may be re-interpreted. However, in a e-voting recount, if it is conducted properly, there is *no* chance that the total vote count for each candidate may change. After all, no actual ballots exist to be re-interpreted. The only matter left is addition, which does not change.

So, in the Guelph recount of 2014, as far as the recount of electronic votes was concerned, June Hofland need not have worried. An identical outcome was assured. I suspect that many people will be surprised to learn this and wonder if this novel sort of recount should be accepted.

E-voting should not be accepted until we, as a society, have had a proper chance to consider and discuss this important change.

For one thing, Guelph's current practice is to apply the traditional sort of recount to in-person voters while applying the novel sort of recount to online voters. This policy is incoherent and, for this reason alone, must be reconsidered.

For another thing, the novel sort of recount seems to have slipped in by stealth. A Google search of the Guelph.ca site for "Internet voting" and "recount" shows that the problem was raised in two comments submitted to the City's Governance Committee (Guelph 2013a). However, no agenda minutes or other documents show that it was discussed by Council. Perhaps the importance of the issue was not understood because the submissions were lacking in any explanations for their claims. I hope that this lack has now been made up for. The change in the meaning and role of recounts for e-voting should not be adopted by stealth but only after due consideration.

Guelph (2013a, July 16) "Addendum, committee agenda: Governance committee." URL: http://guelph.ca/wp-content/uploads/governance_addendum_071613.pdf

Guelph (2014a). "City announces Ward 3 recount results." URL: http://guelph.ca/2014/11/city-announces-ward-3-recount-results/

Conclusion

In conclusion, the e-voting system proposed for use in Guelph does possess the merits of convenience and accessibility. However, it is not likely to increase turnout. Also, it increases risks of fraudulent voting and electoral disruption that would threaten to undermine the legitimacy of the government. Finally, it changes the nature of elections in terms of how they are understood, controlled, and their results interpreted. These concerns are not merely hypothetical but are reflected in experience with e-voting systems.

Many of these issues appear not to have been adequately considered. Some may be mitigated by improvements to the system. Others suggest that e-voting may not be appropriate for general use for some time. As there is also no general, pressing need for e-voting, there is no reason to rush into adopting it. I conclude that the e-voting system proposed for use in Guelph at this time should not be adopted.

Appendix: Recent reports and recommendations on e-voting in Canada

In recent years, four Canadian provinces and the federal government have studied the adoption of e-voting. Each study recommended against it. Links to these reports are provided below.

On March 1, 2017, the *New Brunswick Commission on Electoral Reform* submitted its report to the New Brunswick legislature. The Commission studied the matter of e-voting and made the following recommendation: "The government not proceed with electronic voting at this time, due to concerns related to security, confidentiality and privacy."
URL: http://www2.gnb.ca/content/dam/gnb/Departments/eco-bce/Consultations/PDF/PathwayToAnInclusiveDemocracy.pdf

In December 1, 2016, the *House of Commons Committee on Electoral Reform* studied the matter of e-voting and made the following recommendation to the Parliament of Canada: "The Committee recommends that online voting not be implemented at this time."
URL:
http://www.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&Parl=42&Ses=1&DocId=8655791&Language=E&File=267

On February 1, 2014, The *Independent Panel on Internet Voting* issued its report to the Government of British Columbia. Its main recommendation was: "Do not implement universal Internet voting for either local government or provincial government elections at this time."
URL: http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

On June 1, 2013, the Chief Electoral Officer of Ontario issued his *Alternative Voting Technologies Report* to the Ontario Government. It studied the matter of electronic voting, including e-voting, which it called "network voting," and made the following recommendation: "At this point, we do not have a viable method of network voting that meets our criteria and protects the integrity of the electoral process."
URL:
http://www.elections.on.ca/content/dam/NGW/sitecontent/2014/reports/Alternative%20Voting%20Technologies%20Report%20%282012%29.pdf

On May 6, 2013, the Chief Electoral Officer of Nova Scotia issued his *Elections Nova Scotia: Annual Report of the Chief Electoral Officer April 1, 2012 – March 31, 2013*. In the matter of Internet voting, the Officer made the following recommendation: "And, while most would agree that online voting is consistent with our increasingly online society, the basic questions of how to maintain the security, validity, and integrity of our elections has not yet, in our opinion, been satisfactorily answered."
URL: https://electionsnovascotia.ca/sites/default/files/ENS%20AR%20Web%202012_13.pdf

Since 2006, the Province of Quebec has maintained a moratorium on electronic voting of all kinds in light of previous experience with the technology.
URL: http://www.electionsquebec.qc.ca/english/municipal/media/electronic-voting.php

My name is Jason Dodge and I am here as a representative of the Guelph Accessibility Advisory Committee alongside our Chair, Brad Howcroft.

The City of Guelph Accessibility Advisory Committee recommends that the online voting option be available for the advance polls as well as on Election Day for the 2018 municipal election. During the 2014 municipal elections people with a disability were thrilled to be able to cast their vote online. For many people with a disability this service meant that for the first time, they were able to vote independently. Those of us without a disability rarely realize how important it is to be able to carry out a task by one's self, especially one so important.

There has been speculation that online voting had no impact with the noticeable increase of voter turnout in 2014. Standing here tonight I can attest that this speculation is incorrect. The online option allowed my own brother, Will Dodge, to vote for the first time in his adult life. He believes in his right to keep his vote confidential and a number of health and wellness factors had previously prevented him from being able to reach the poll stations.

Will is extremely proud to have voted independently in 2014. To remove the online option will automatically put up a huge barrier; a barrier that will result in Will, and many others in Guelph like him, being unable to exercise his ability to vote in 2018.

Accessible online voting is an important part of an inclusive suite of options that ensures all residents have an equal opportunity to vote during a municipal election.

The Guelph Accessibility Advisory Committee understand the concerns regarding security of the Municipal Property Assessment Corporation's (MPAC) voter list as it pertains to online voting however we believe that regardless of the method of registering voters, there is a risk that fraud can take place. After a presentation by Stephen O'Brien, the City Clerk, last Tuesday during our advisory committee meeting, the AAC members trust that City Clerks understand their responsibility under the Municipal Act and will apply the needed measures to mitigate the voter list risks that have become a concern for some. Further the committee feels that there is more risk involved if the most accessible voting experience for the citizens of Guelph, which would be a true democratic experience for all, is not offered as this could be seen as an accessibility related accommodation.

The Accessibility for Ontarians with Disabilities Act requires municipalities to take into account the needs of people with a disability when providing a service. Accessibility planning is a key theme throughout this legislation. Staff did their due diligence when planning for the 2014 elections as they worked with the AAC to test the online system for accessibility. Staff members continue to include accessibility into their planning by encouraging the option of online voting for 2018. It is felt that this work along with the measures that the Clerk's office will have in place to mitigate fraud risk have positioned the municipality to offer a fully integrated and barrier free voting experience in 2018. We request that when making your decision on this topic that you consider voters with a disability who were able to vote online in 2014. It would be a dis-service to silence these votes because of a perceived fear of fraud.

Brad Howcroft AAC Chair and Jason Dodge AAC Member