COMMITTEE AGENDA

CONSOLIDATED AS OF JULY 12, 2013

TO	**Governance Committee**
DATE	July 16, 2013
LOCATION	Council Chambers, Guelph City Hall, 1 Carden Street
TIME	3:00 p.m.

DISCLOSURE OF PECUNIARY INTEREST AND GENERAL NATURE THEREOF

CONFIRMATION OF MINUTES – February 11, 2013 open meeting minutes

PRESENTATIONS (Items with no accompanying report)

None

CONSENT AGENDA

The following resolutions have been prepared to facilitate the Committee's consideration of the various matters and are suggested for consideration. If the Committee wishes to address a specific report in isolation of the Consent Agenda, please identify the item. The item will be extracted and dealt with separately. The balance of the Governance Committee Consent Agenda will be approved in one resolution.

ITEM	CITY PRESENTATION	DELEGATIONS	TO BE EXTRACTED
GOV-2013.8 2014 Municipal Election: Methods of Voting	• Blair Labelle, City Clerk • Nicole Goodman, Research Consultant	• Janet Doner, Manager Community Engagement & Global Citizenship, Student Life, University of Guelph • Tyler Valiquette, Local Affairs Commissioner, University of Guelph Correspondence: - Chris Cates - David Fishback - Sonny Sorensen - Barbara Mann	√

GOV-2013.9 CAO Performance Appraisal Committee Terms of Reference and Process Protocol			
GOV-2013.10 Delegation of Authority for Operational Applications, Contracts and Agreements			
GOV-2013.11 Outstanding Motions of the Governance Committee			

Resolution to adopt the balance of the Governance Committee Consent Agenda.

ITEMS EXTRACTED FROM CONSENT AGENDA

Once extracted items are identified, they will be dealt with in the following order:

1) delegations (may include presentations)
2) staff presentations only
3) all others.

STAFF UPDATES & ANNOUNCEMENTS

ADJOURN

NEXT MEETING – September 16, 2013

Mayor Farbridge and respected councillors for the City of Guelph,

My name is Chris Cates and I am a citizen of Canada living in the city of Edmonton. Recently, I have heard news that your city is considering using internet voting in the next election. While I am not a resident of your city, I am very much concerned about the use of internet and electronic voting used anywhere in Canada because of the great harm it can do to our democracy.

Many municipalities across Canada are exploring the idea of using online and electronic voting solutions and some have already implemented the use of these technologies. While the **idea** of internet voting has a numerous merits, such as allowing disabled or infirm people the ability to vote, the practical application of internet voting is filled with numerous technical problems to which there are no solutions. I am writing you today to make you aware of the risks associated with using an online voting system.

Advocates, city clerks, and sales representatives will try to convince you that electronic voting will save your city money and increase voter participation. They will try to tell you that online voting is as safe and secure as online banking. Some advocates will even go so far as to lie by saying there have never been any problems with internet voting. These statements simply are not true as proven recently by the electronic election held in France where journalists, not hackers, were able to breach the election system promoted as “fraud-proof” and “ultra secure” (http://www.independent.co.uk/news/world/europe/fake-votes-mar-frances-first-electronic-election-8641345.html).

Attached to this message is the staff report from the city of Kitchener who recently performed an 18-month study into the use of internet voting. In this report you will find their study concluded that internet voting doubled election costs and only marginally increased voter turnout. The report also brought up serious concerns about the security associated with the use of internet voting.

In a recent CBC news broadcast with journalist, Rob Wipond, the internet voting system used in the Halifax Regional Municipality (HRM) during their last election was found to be filled with numerous security holes (http://www.cbc.ca/informationmorningns/2013/06/17/security-worries-over-website-used-during-halifaxs-last-election/). Computer security researcher, Kevin McArthur, found the system was vulnerable to man-in-the-middle types of attacks where elections officials and the internet voting company would have no idea the election was hijacked (http://www.unrest.ca/setting-the-record-straight-on-halifax-election-evoting).

Many advocates and news agencies report the same old saying: "If we can bank online, why can't we vote online?" Banking online means a trust must be formed between you and the bank. When logging into the bank's system, you know the bank and the bank knows you. Voting means your identity must remain 100% secret and there must be nothing linking you to your ballot. Would you bank online if your identity was to remain completely confidential from the bank? Likely not. These advocates also do not tell you about the numerous viruses which have circulated the world and scammed millions of dollars from banks. Viruses like: Zeus (http://en.wikipedia.org/wiki/Zeus_(Trojan_horse)) and SpyEye (http://www.dailymail.co.uk/sciencetech/article-2083271/SpyEye-trojan-horse-New-PC-virus-steals-money-creates-fake-online-bank-statements.html)

Advocates and supporters of electronic voting will also tell you that the system is full auditable, but nothing could be further from the truth. There is no way to independently audit an electronic election. Recounts are not possible. The e-voting system will only produce the same numbers it did before. What if there was a glitch which caused votes to be flipped from one candidate to another (http://tv.msnbc.com/2012/11/06/machine-turns-vote-for-obama-into-one-for-romney/)?

What if there was a mathematical error in the code which caused the election results to be miscalculated (http://www.freemalaysiatoday.com/category/nation/2013/01/05/dap-election-fiasco-an-embarrassment/)? There is no way to verify the election results because all votes are digital.

You may find it interesting to know the most outspoken individuals protesting the use of internet voting are computer science experts. These individuals are speaking out publicly and proving the technology cannot be trusted with our democracy. Computer experts like Prof. Ronald L. Rivest Ph.D. who is co-founder of the RSA security encryption algorithm and VeriSign used in many of today's online transactions. Or, Assc. Prof. J. Alex Halderman Ph.D. who successfully hacked the proposed Washington D.C. internet voting system which, were it not for his efforts, was about to be used in an actual election a mere 2-3 weeks later.

In 2012-13 the city of Edmonton explored the idea of using internet voting for its upcoming municipal election. A citizen jury was formed and a mock "Jellybean" election was conducted to test the internet voting system. All of the news reports of the time reported the system being safe and secure and no problems were found. As you may or may not be aware, I protested against the use of internet voting here in Edmonton in the rest of Alberta. My efforts helped raise awareness of the numerous flaws which exist with internet voting. Some of these flaws were highlighted by my ability to cast **two** ballots completely undetected by the online voting system or the election officials. After raising my concerns and highlighting the numerous risks associated with internet voting Edmonton city councillors voted 11-2 against using the technology.

Shortly before their decision I wrote a letter to Alberta Municipal Affairs Minister, Honourable Doug Griffiths, which further explained how internet voting does not uphold key election principles when used. It wasn't long after the city of Edmonton rejected using internet voting that Minister Griffiths sent a letter to all municipalities stating internet voting was not going to be allowed in Alberta. I have attached the letter to this message for your consideration.

I implore you to read the attached report and letter and I am sure that when you do, you too will find that internet voting does not enhance our democracy. With the use of internet voting citizens can no longer trust our elections. Performing recounts or proper independent audits become impossible as there is no way to independently verify the ballot was received exactly as it was cast. There is no way to ensure that voter coercion, vote buying/selling did not take place, or the system wasn't compromised by an individual or group with an agenda to manipulate the election results. There is no way to ensure that a virus or other malware didn't infect the system to change the results. There is no way to ensure the virtual ballot box wasn't virtually stuffed with ballots or switched for another virtual ballot box. There is no way to prevent a Distributed Denial of Service (DDoS) attack like the NDP election, or stop a phishing site from tricking users into submitting their ballots on a fake election server. By the way, to this day the culprits responsible for the NDP DDoS attack have never been identified or prosecuted, and the NDP had to call off their investigation due to enormous costs of investigating the crime (http://www.countingthevote.ca/apps/blog/show/21700105-pov-a-look-back-on-the-scytl-ndp-internet-voting-debacle). Is this what is waiting for your next election?

By deciding against internet voting you are upholding democracy in Canada and sending a message that this technology is not ready for use in our elections. We should not be using our elections as testing grounds for private for-profit voting companies. Internet voting companies claim their systems cannot be hacked and can withstand any cyber-attack. But I retort by asking you this: if secure government organizations like CSIS, the FBI, and numerous financial institutions can't stop hackers from penetrating their systems, what makes you think an internet voting company can?

Many municipalities have rejected the use of online voting because it does not live up to expectations. The city of Kitchener rejected using internet voting along with the city of Edmonton and recently the city of Thunder Bay (http://www.tbnewswatch.com/news/286546/Rejected). The provinces of Alberta and B.C. have rejected using internet voting. Huntsville, Ontario returned to using paper ballots after experiencing a significant problem during their 2010 internet election.

To learn more about internet voting and the risks associated with it, please visit my web site: http://www.countingthevote.ca. There are too many risks associated with using any electronic voting system. Please help to protect our democracy by using an open, transparent, and auditable election method that is proven successful: Paper ballots!

Regards,

Chris Cates, Computer Expert
CountingTheVote.ca

KITCHENER

Staff Report

Finance and Corporate Services Department

www.kitchener.ca

REPORT TO:	Finance & Corporate Services Committee
DATE OF MEETING:	December 10, 2012
SUBMITTED BY:	R. Gosse, Director of Legislated Services/City Clerk
PREPARED BY:	R. Gosse - 2809
WARD(S) INVOLVED:	n/a
DATE OF REPORT:	November 2, 2012
REPORT NO.:	FCS-12-191
SUBJECT:	ALTERNATIVE VOTING – INTERNET VOTING

RECOMMENDATION:

For information and discussion.

EXECUTIVE SUMMARY:

This report looks at the use of internet voting and attempts to answer the question of whether or not internet voting should be introduced as a voting option for the 2014 elections. Staff is of the opinion that it should not be introduced in 2014 based on several factors outlined in greater detail in this report such as:

- Security of an internet voting system;
- Data that suggests it does not increase voter turnout and in particular, younger voters;
- Does not meet all of the principles of a democratic voting process;
- Cost;
- The lack of overarching guidelines especially in the area of voting system security and,
- The absence of a Canadian legal challenge to this voting method.

BACKGROUND:

In June 2011, Council directed staff to report back in 2012 on alternative voting methods and in particular, internet voting and the option of implementing this type of voting for the 2014 municipal elections. This report will focus mainly on internet voting being it is a completely new method of voting for the City of Kitchener.

REPORT:

Internet voting is becoming more prevalent within Ontario and other jurisdictions across Canada and around the World. It is a voting method that allows a voter to submit a digital ballot over the public Internet utilizing a web browser or application through a PC, tablet or smart phone. This voting method provides a great deal of convenience by allowing voters with internet access to vote from any location at any time during the voting period. It is also provides access to the voting process for many voters with a disability.

Despite the apparent conveniences of internet voting, there are risks involved. It is critical that elections are conducted with utmost integrity and in compliance with democratic principles. In order to maintain public confidence elections should be accessible, transparent, secret, accountable and secure from fraud. Internet voting may not adhere to some of those principles raising the question of whether or not it is important enough to dispense with one or more principles for the sake of convenience and other possible positive outcomes. It is important that decisions with respect to introducing internet voting, take into consideration the need to balance these competing principles.

This report will attempt to bring together information from various papers, reports, data and documents on the subject to assist council in making a decision on whether or not, internet voting is an acceptable and appropriate voting method for the City of Kitchener to introduce in 2014.

The Internet Voting Experience

Internet voting has been trialled over the past decade by several countries and jurisdictions throughout the world. In all cases except one, this voting method has only been offered on a local or jurisdictional level, not on a national level. In addition, except for some Ontario municipalities in 2010, internet voting has been offered as a voting option along with others such as paper ballot, phone voting and mail-in; in other words, internet has not been the sole method of voting.

Europe and Australia

Several European countries have investigated and piloted internet voting and Estonia and Switzerland appear to have embraced this method having conducted several elections with internet voting as an option. Estonia is the only country to have offered internet voting on a national level. Norway conducted its first pilot in 2011 on a limited municipal level and pending the outcome of an extensive post-election report, there are plans to introduce internet voting on a national level in 2017.

Germany, the Netherlands and the United Kingdom have used electronic counting equipment and have trialled internet voting but all three have moved away from these voting options based on certain democratic voting principles not being met. Both Germany and the Netherlands have gone so far as to decommission all electronic voting methods citing lack of transparency, accountability and the fact that equal and free voting could not be verified. The United Kingdom also cited transparency and security issues and found that the majority of internet users would have voted using the other available methods raising questions with respect to cost and value.

Australia piloted internet voting in 2007 but deferred further trials in 2009 citing cost as the major impediment in offering this voting option.

North America

The United States have trialled internet voting but only in limited uses such as primaries and overseas/military voters. Security and risks to voting integrity have been cited as concerns and as such, no internet program has been established on a federal level. According to one researcher, a national policy on internet voting is not expected in the near future. Certain individual States have used internet voting again mostly for military and absentee voters however; security remains an issue with some and there is evidence that a few states are moving back to a paper ballot to be counted either manually or by optical-scan machines.

In Canada, the Federal and several Provincial governments have commenced their investigations into the use of the internet as an optional method of voting. On the federal level the Office of the Chief Electoral Officer has completed the terms of reference for internet voting and if approval is given, will offer the option for a by-election in 2013. It is also expected that if the pilot is considered successful, a federal policy on internet voting including security and integrity, will be developed sometime in 2015-16. This is much the same for the Ontario government with a goal to pilot the option in 2012 and report back to the Speaker of the House in 2013.

The Alberta and Nova Scotia provincial governments have taken steps to allow piloting of internet voting on both the provincial and municipal levels. Edmonton has conducted a mock vote using the internet and Halifax and a few smaller towns have conducted elections with internet as an option and Halifax is again offering this method for the current 2012 elections.

Ontario

Internet voting was first introduced by the Town of Markham in 2003 and has continued to be an option in the 2006 and 2010 elections. In 2006, several more municipalities offered internet voting and in 2010, 44 municipalities that completed a survey for the Association of Municipal Managers, Clerks and Treasurers of Ontario, indicated use of the internet. Of the 44 municipalities, 6 offered internet as an option and only for advance voting, 8 offered internet as an option including election day and, 30 as the only means of voting along with telephone voting. It should be noted that the 30 municipalities that offered only electronic voting (internet and telephone), the largest in population was approximately 30,000; most were under 15,000.

Results and Outcomes

Throughout most internet voting trials around the world, one factor has become clear; the majority of citizens have generally accepted internet voting as a practical option. This is not to say the majority of citizens embraced the technology rather, they viewed it as an acceptable alternative.

Although it has been found that voters have accepted internet voting as a method for casting votes, there is no evidence to show it increased voter turnout. This is true throughout most, if not all, internet voting trials.

The Town of Markham has been a front-runner in this field, being one of the first jurisdictions in the world to introduce internet voting in 2003. The Town has offered this voting method as part of the advance voting period for the past 3 regular elections and following each election, they contracted a third-party company to undertake an extensive follow-up to assess the effectiveness and value of internet voting.

The follow chart shows the Town of Markham turnout over the 3 years that internet voting was available during advance voting.

	2003			2006			2010
Electors	158000			164500			185470
Turnout	42198			61948			65927
% turnout	26.71%			37.66%			35.55%
internet votes	7210			10639			10597
% internet of turnout	17.09%			17.17%			16.07%
% internet of electors	4.56%			6.47%			5.71%

The post-election analysis undertaken by the consultant for the Town showed that whereas advance voting increased dramatically, 300% in 2003, the overall turnout did not increase significantly. It should be noted that 2003 was a particularly low turnout whereas 2006 and 2010 were closer and perhaps slightly higher than the average turnout for the Town. The consultant's report which included post-election surveys amongst those who utilized internet voting showed that approximately 75% of those using the internet had voted in the previous election and had indicated they would have voted regardless of voting options. This was true in each of the 3 elections however; alternatively, 25% of the voters indicated they did not vote previously showing that the method may attract new voters. In addition, acceptance of those using the internet was very high, not only in Markham but for most other jurisdictions globally. Most respondents indicated they would use the internet in future elections.

The figures from the Cities of Peterborough and Burlington are similar to that of Markham's.

	City of Peterborough				City of Burlington
	2006		2010		2010
Electors	52116		54874		121525
Turnout	25036		24219		45671
% turnout	48.04%		44.14%		37.58%
internet	3473		3951		2500
% internet of turnout	13.87%		16.31%		5.47%
% internet of electors	6.66%		7.20%		2.06%

The 2011 elections held in Norway trialled internet voting for some municipalities which allowed for comparison between those with and without internet voting as an option. The post-election analysis showed clearly that internet voting did not have a positive impact on turnout; the results from those municipalities mirrored the results from municipalities without the internet option. The report also indicated that 89% of internet voters surveyed stated they would have voted if internet voting was not available.

The Town of Markham post-election analysis went beyond just looking at voter turnout; it also included a breakdown by age groups for those who used the internet to cast their vote.

voters by age									
	2003			2006			2010*		
18-24	9%	649		7%	745		18-19	2%	219
25-34	12%	865		11%	1170		20's	11%	1134
35-44	22%	1586		22%	2341		30's	13%	1380
45-54	27%	1947		28%	2979		40's	23%	2412
55-64	19%	1370		21%	2234		50's	26%	2781

64+	8%	577		11%	1170		60's	17%	1827
Unknown	3%	216					70's+	8%	844
	100%	7210		100%	10639			100%	10597

*Note: The Town changed the age groups in 2010.

The results by age groups in Markham are very much the same as in other jurisdictions around the world. In all cases where post-election follow-up was conducted, it was found that the largest users of the internet were by voters age 45 to 55 and the smallest groups were 18-34. In Norway a focus group of teenaged voters was undertaken and it was found that the younger voter viewed walking to a poll to cast a ballot as ceremonial and symbolic of adulthood. They also indicated that it was more important to ask why a young person should vote rather than what method they will use to vote. There is clear evidence that, regardless of geography internet voting does not attract younger voters.

Security, Scrutiny and Auditability

Internet voting does have risks especially in the area of software/hardware security which is one of the main reasons given by opponents of internet voting. Although there is a risk, there is no evidence that a government election utilizing the internet has ever been hacked or suffered a cyber-attack. That is not to say no internet voting system hasn’t been hacked, there are several cases of such attacks taking place during a pre-election period when outside persons and groups were invited to test the security of a system.

A security attack on an internet voting system can take place in basically 2 ways: hacking into the servers and; denial of service whereby multiple computers on the internet receive instructions to attack the web site hosting the voting system, essentially overloading and shutting down the web site. Although these risks are real and attacks have taken place, with today’s ever evolving security software, the risk is low that a system can be totally compromised.

Another cyber-attack method which could be more detrimental to the voting process and integrity of a voting system is one that does not attack the municipality’s servers but rather, attacks the voter’s computer. Spyware or another type of intrusive software can be inadvertently downloaded onto a private PC or one that is used by the public such as those available in libraries or cyber-cafes. Once downloaded the hacker could introduce software to change how the voter casts their votes. The important issue here is the fact that no matter how well the servers are protected, there is no way to ensure that the voter’s choice has been received correctly. Once again, the risk of this method of attack is considered extremely low especially when it’s a municipal election but, it can raise some concerns adding to the public perception that the system is not fool-proof.

The largest impact on an election stemming from security issues is not necessarily the integrity of the system but the cost involved to ensure the system is secure and to satisfy the public and candidates as to any concerns they may have. It is extremely important that the public has complete confidence in any voting system; a lack of confidence may result in lower voter turnout and/or post-election challenges.

In order to mitigate these issues, a Request for Proposal to provide an internet voting system will have to include proof that the system is secure and is certified to certain standards. However; without a Canadian standard, the City would have to decide on an appropriate standard either from another jurisdiction (i.e. Europe) or in consultation with a third-party digital security company. It is assumed that the costs incurred by companies offering internet voting systems to undergo such a security assessment will be passed along to municipalities. In addition, once a system is chosen and put into place, the municipality must have a security consultant test and verify the integrity of the entire system including hardware. It may also be prudent to have a post-election security audit to ensure and provide proof that the system was not compromised (i.e. no programming code was added during the election).

There is one indisputable fact regarding internet or other Direct-Recording Electronic (DRE) voting system that cannot be ignored; it is the lack of auditability and the inability to re-create the vote. A paper ballot based system regardless how the ballots are tabulated maintains a means of recreating the vote should a recount be ordered. Since a DRE system does not produce a paper copy of any vote, a recount would rely solely on an audit of the system (so many votes received and so many votes counted). This inability to recount votes could be a real issue should an election be challenged and end up in the courts. It is also one of the main reasons that several European countries decided to decommission their DRE systems and not move forward with internet voting. Scrutiny of the election process was another reason.

One of the tenets of a democratic and free election is the ability for the public to scrutinize the process ensuring full transparency. This is even more important for candidates who may appoint scrutineers to observe and ensure the voting process is properly carried out. When voters can cast their vote away from the public eye, it raises questions on whether or not that part of the process is taking place properly and without coercion and/or fraud.

Cost

Holding elections is the basis for our democratic society and therefore costs should not be a factor, however; like everything undertaken by the City, costs must be taken into consideration. The operation of an election should balance cost with convenience to the elector therefore cost to add internet voting as an option should be weighed against the added value it may bring.

In 2010 the cost of holding the elections in Kitchener was approximately $360K made up of: hiring workers, leasing equipment/software, postage and supplies. In 2010 the cost of holding elections in Markham, a municipality with about 25% more electors, was approximately $1.2M.

The current estimated budget for 2014 is $390-$400K without adding internet voting as a voting option. Should internet voting be introduced in 2014 the following chart shows the estimated additional costs to be added to the current budget:

Internet Software	$1.50 - $2.00/elector with estimated 158,000 electors in 2014	$237K - $316K
Postage	Additional postage required; each notification will now be mailed individually rather than grouped by address	$25K
Security Audit	3rd party audit of entire internet system	$10-20K
Promotion	To ensure success, extensive promotion will be required (Markham costs in 2010, $216K)	$50-75K
Total Internet Voting	Total estimated costs using lowest costs in a range	$322K

Current Budget w/o internet voting	Current budget lowest costs to run an election similar to 2010.	$390K
Total 2014 Budget with Internet voting	Total estimated lowest cost with internet option	$712K

Elections are paid out of a reserve that is built up with annual contributions over the 4 years between elections. If internet voting is to be offered in 2014, the current annual contribution to the election reserve will have to be increased by $175-200K in budget years 2013 and 2014 to ensure the additional $300-$400K is available. This will increase the total contribution for the 2 years from $90K to $265-$290K. Should internet voting continue past 2014, then the annual contribution would be reduced so that each year equals 25% of the projected election costs for 2018. The estimate for the contributions between 2014 and 2018 is $200/annum. It is noted that the election reserve also receives interest revenue during the 4 years.

CONCLUSION:

Internet voting has been offered as a voting option since the late 1990's in various jurisdictions around the world, however; the number of countries/jurisdictions that continue to offer internet voting as an option is relatively small. Ontario is one jurisdiction that has seen a steady increase in the number of municipalities offering internet voting albeit; the majority of municipalities are considered to be small with populations less than 30,000.

Where internet voting has been offered, data suggest it has been well accepted by the public as an alternative voting method, however; there is no clear indication that it increases voter turnout. There is data that shows internet voting does not increase voter turnout amongst younger voters.

Security issues are a real threat but most studies conclude that the risk is small to medium. Notwithstanding the risk level, security standards should be in place to ensure public confidence in the election process. It is anticipated, but not guaranteed that the federal government will develop such standards by 2015-16.

Internet voting is very convenient allowing voters the opportunity to vote anywhere at any time during the voting period. Data compiled as part of several post-election studies where internet voting was being piloted showed that the majority of internet users would have voted regardless if internet voting was available or not. Internet voting also offers some voters with a disability the ability to access and participate in the voting process without assistance. This is not the only method to allow accessible voting, there are other methods using paper ballots or touchscreens.

Prior to introducing an internet voting option, consideration must be made with respect to this voting method and how it meets or doesn't meet the democratic principles of an election. There is a lack of transparency and scrutiny when voters are allowed to vote without public oversight that ensures the vote has been cast fairly and without coercion or fraudulently. This is particularly significant for Kitchener in light of the 2010 Ward 9 race that resulted in a 1 vote difference and subsequent recount.

The cost to offer internet voting as one option for electors is significant and cannot be ignored. The estimated cost will double the election budget for 2014 yet, data from other jurisdictions indicate it may not increase voter turnout enough to justify the cost.

In light of the issues raised with respect to internet voting as an additional voting option, it is staff's opinion that it should not be introduced in the City of Kitchener for the 2014 municipal elections. The earliest election that internet voting should be considered is 2018 by which time it is anticipated security standards will be in place. One event that has not taken place in Canada as of yet that may assist in answering questions regarding security and election principles, is a court challenge. It was a court challenge in Germany that resulted in that country abandoning any further internet voting and the use of DRE voting systems. A challenge in Canada may set the legal parameters for offering internet voting and answer the question with respect to the importance of election principles in context of voting convenience.

ALIGNMENT WITH CITY OF KITCHENER STRATEGIC PLAN:

Efficient and Effective Government: Exploring technological changes to ascertain its appropriateness in enhancing community access to the election process. Positioning the City as a leader in public sector processes; ensuring accountability and transparency.

FINANCIAL IMPLICATIONS:

Financial implications are dependent on whether or not internet voting is going to be offered in 2014. It is estimated that the addition of internet voting as a voting option will add between $325K and $400k to the current budget of $390K.

COMMUNITY ENGAGEMENT:

A draft of this report is to be presented to Compass Kitchener on December 5th for questions and feedback. Compass Kitchener has been looking into voter engagement and turnout including internet voting as an option. The outcome of that meeting will be reported on verbally at the December 10th Finance & Corporate Services Committee meeting.

ACKNOWLEDGED BY: D. Chapman, DCAO – Finance & Corporate Services Department

Chris Cates
111 Royal Terrace
Edmonton, Alberta T6J 4R2
Canada

February 1, 2013

Honourable Doug Griffiths
Minister of Municipal Affairs
18th Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta T5J 4L4
Canada

Mr. Paul Whittaker
Deputy Minister of Municipal Affairs
18th Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta T5J 4L4
Canada

Dear Honourable Mr. Griffiths and Mr. Whittaker,

My name is Chris Cates and I am a Canadian citizen residing in Edmonton, Alberta. As you are already aware, the City of Edmonton held a mock election in October/November of last year. This mock election was to test the concept and readiness of Edmonton and other municipalities using internet voting as an option for voters to cast ballots in the upcoming 2013 municipal election.

I am writing you today to express my concerns with local municipalities and the provincial government of Alberta exploring the idea of using internet voting for their elections. As a computer programmer and former network administrator with over 20 years of experience in the Information Technology (IT) industry, I am well versed in the various methods organizations can employ in attempts to keep their network as secure as possible. However, this experience has also shown that, despite our best efforts, no network can be completely secure from intrusion.

In the letter written by Mr. Whittaker, dated October 19, 2012, to Mr. Simon Farbrother, City Manager for the City of Edmonton, Mr. Patrick Draper, City Manager for the City of St. Albert, and Mr. Kevin Glebe, Intrim Chief Commissioner for Strathcona County, support for the use of internet voting in the next municipal election will only be provided as long as the following principles are met:

- Maintain or enhance accessibility of voting opportunities;
- Ensure only eligible electors can vote;
- Ensure eligible electors can vote only once;
- Ensure that voters will have the opportunity to vote in private;
- Ensure that each voter's choices cannot be associated with the individual voter;
- Ensure that reasonable measures are in place to protect the security of votes and the voting system;
- Ensure that the process is subject to adequate audit and verification; and
- Identify measures to be taken to promote transparency and reliability, including the use of communication or education programs to make voters familiar with the process and safeguards, or through the use of audit procedures and the publication of audit results.

I would like to take a moment of your time to explain how many of the listed principles are not met and cannot be met using internet voting or electronic voting as an option in an election. I will detail this information by using the points listed above.

Maintain or enhance accessibility of voting opportunities

Internet voting enhances accessibility of voting by providing people who are elderly, infirm, disabled, or abroad at the time of an election a means of voting without needing to visit a local polling station. By making use of the internet people can access the proposed online election system from almost anywhere in the world by using a web browser on an internet enabled device (i.e personal computer, laptop, smart phone, etc.).

However, this statement does not take into consideration the very real possibility of an online election being disrupted by a Denial of Service attack or other cyber attack. During the NDP leadership race in March 2012, Scytl's election system was disrupted by a Distributed Denial of Service (DDoS) attack which prevented many voters from casting ballots. During the attack legitimate voters both at the NDP convention hall and others across Canada could not log in to the election system. At one point, Scytl had to lock out remote voters so only those at the convention hall were allowed to vote.[1] One couple, John & Sandra Wilson spent the entire day trying to vote and were unsuccessful. After they entered their PIN code a message would appear on their screen saying their time had expired or that they had already voted. [2]

In the likely event of an internet voting system becoming a target of a Distributed Denial of Service attack, how many voters will be unable to cast their ballots? How many voters will it take before the election is called and a new election will need to be held? How much of taxpayer money will be spent investigating this type of attack? In the case of the NDP attack, neither Scytl nor the NDP were ever able to prove who attacked the system and to this day no one has ever been prosecuted.

[1] Huffington Post, March 24, 2012 – Vote Fail: NDP Online Ballot Issues Tied To Attempted Cyber-Attack (http://www.huffingtonpost.ca/2012/03/24/vote-fail-ndp_n_1377134.html)

[2] Toronto Star, Saturday March 24, 2012 – NDP Leadership: Voting Delays Caused By 'Outside Interference' (http://www.thestar.com/news/canada/2012/03/24/ndp_leadership_voting_delays_caused_by_outside_interference.html)

Ensure only eligible electors can vote

In order for any municipality to ensure only eligible voters can cast a ballot in an election, a database of registered voters must be created, maintained, and secured. Currently, Edmonton and other municipalities do not have a database of registered voters as this database becomes outdated the moment it is created due to the number of people moving in and out of the city or province. The only option left is for voters to register at the start of an election, leaving the possibility of a person or a group to create a number of false identities to gain the ability to cast multiple ballots.

In a paper ballot election, voters must register and provide government issued photo identification to cast their ballot. In an online election the same is also true. Voters must register by providing their name, address, e-mail address, etc. and a scanned copy of government issued photo identification.[3] Where the two systems differ is when it comes time to cast a ballot. If a malicious person wanted to create numerous fake identities to cast multiple ballots there is a good chance this person would be detected at the polling stations, and spend most of his/her time travelling or waiting in line to vote. The possibility of a single person being able to cast hundreds of paper ballots without being detected is not very likely. However, during an online election a single person could use an image editing program (i.e. Photoshop) to create multiple false identities and cast hundreds of ballots. By casting those ballots at publicly shared computers (i.e. library, internet cafes, etc.) the possibility of being detected is quite slim, and the results of the election could easily be affected.

Ensure eligible electors can vote only once

As I am sure you are already aware it is completely possible for someone to cast more than one ballot during a paper ballot election. However, paper ballot elections provide a means of identifying this type of voter fraud as a paper trail exists for investigators to follow and catch the perpetrator.

As it was pointed out in the previous section it is not a complicated task for a single person to cast multiple ballots during an online election. However, this is not the only method which could be employed to allow a person or group to influence the outcome of an online election.

In October 2010, Peter Byvelds, of Brinston, Ontario, was able to cast five ballots during an online election. [4] Byvelds was able to do this by stealing the PIN codes of four family members and casting their ballots in addition to his own. [5] During the 2012 mock Jellybean election here in Edmonton, Alberta, I was able to use a different method to cast more than one ballot as well. This information was reported to the Centre for Public Involvement, who was tasked with reporting public readiness of internet voting, during one of their roundtable meetings but was not reported to Edmonton City Council by either the Centre for Public Involvement or the city clerk. I therefore brought the matter before Edmonton City Council during an Executive Committee meeting on January 28, 2013.

[3] City of Edmonton, No Date – Internet Voting FAQ (http://www.edmonton.ca/city_government/municipal_elections/internet-voting-frequently-asked-questions.aspx)

[4] CBC News, March 8, 2011 – Ont. Man Cast More Than One Vote In Election: OPP (http://www.cbc.ca/news/canada/ottawa/story/2011/03/08/ottawa-voting-charges.html)

[5] 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)

Furthermore, internet voting creates a means for proxy voting to take place. As I am sure you are already aware this is when someone can cast a ballot on someone else's behalf, and is not legal in our current elections. An online election also introduces the possibility for an underground movement to be established which would facilitate a means for votes to be bought or sold. In a paper ballot system this may be possible but it is unlikely to happen as there is little means for the voter's ballot to be recorded.

Ensure that voters will have the opportunity to vote in private

While internet voting does provide a means for a voters to be able to cast ballots from their home, work, smart phone, etc. it does not necessarily mean their vote is cast in private. The very nature of sitting at a computer or using a smart phone to cast a ballot means the voter can easily be removed from the public eye. As you know, a polling station only allows one person to be at a polling booth at one time unless special circumstances require voter assistance. When a voter is at home or at work casting their ballot a very real possibility exists that other people (i.e. spouse, family member, employer, etc.) could be standing behind them coercing the voter to cast a ballot for a specific candidate.

Ensure that each voter's choices cannot be associated with the individual voter

As mentioned previously, in an online election the voter must register with the election system by submitting their name, address, e-mail address, etc. and scanned copy of their government issued photo identification. Once the voter has been approved by the election system, an e-mail message is sent to the voter which contains the PIN code the voter must use to cast their ballot. Each PIN code must be unique in an attempt to maintain one person, one vote.

This is where the fundamental flaw related to electronic voting resides. The PIN code provided by the election system is the code which connects the voter to their ballot. Unlike in a paper ballot system, electronic ballots are marked by a unique code. Internet voting companies will be very adamant at stating the PIN code does not make this connection. The only way to verify this is to inspect the internet voting company's software (source code) and fully review their databases used in an election, which is something they will not allow. Instead, they ask the public to blindly trust this link does not exist.

In 2008, the Finnish government piloted an electronic election to test Scytl's e-voting system. After the pilot was over Electronic Frontier Finland (Effi), a non-profit organization, released a report based on the audit of the election system. In their report they made the following statement:

> *"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"* [6]

[6] 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)

It was also reported:

> *"The auditors said that a group of insiders could in theory create a second ballot box and count the votes from that ballot box instead of the real one."*

During an election, officials responsible for overseeing the election would have been provided decryption keys used to unlock the virtual ballot box, but the electronic voting company would also have access to those same keys. Not only does this constitute a real threat to voter secrecy it also shows that elections can be rigged to favor a specific candidate.

At the end of the election it is the responsibility of the election company to destroy all data associated with the election once it has been certified by election officials. Again, we are asked to blindly trust that this data has been permanently destroyed and is not being kept on a back-up tape, hard drive, or any other media which could be used to retrieve and review the election data at a later date.

Ensure that reasonable measures are in place to protect the security of the votes and the voting system

Once the ballot is cast in an online election any number of circumstances could take place to change the digital ballot including but not limited to:

- The ballot could be changed by a virus or other malicious malware residing on the voter's personal computer prior to it being transmitted to the election server
- The ballot could be lost during transmission and never received by the election system
- The ballot could be captured during transmission to the election system and altered
- Similar to Robo-calls, where voters were directed to alternate polling stations, voters could be mislead or tricked into voting on a fake election server where their PIN codes and passwords are gathered and then used to cast ballots for a specific candidate
- A programmer working for, or previously worked for, the election company could have implemented code or left a backdoor into the election system to allow them remote access to the election system so ballots can be changed
- Systems administrators of the election company could have logged in to the system during or at the end of an election and changed or removed ballots, or, as stated previously, set up an entirely separate ballot box
- A computer hacker or 'hactivist' group could have penetrated the security of the election system and altered ballots to change the results

Makers of online voting solutions claim to have the Holy Grail of internet security and say their system cannot be penetrated. It is a very bold statement for any company to make considering corporate web sites, which hold confidential personal information, like Google[7], LinkedIn[8], and Facebook[9] have been hacked along with secure networks like the Pentagon[10], CIA[11], and the Canadian government[12] to name a few.

[7] Wired, January 14, 2010 – Google Hack Attack Was Ultra Sophisticated, New Details Show (http://www.wired.com/threatlevel/2010/01/operation-aurora/)

[8] CBC News, June 6, 2012 – LinkedIn Confirms Some Users' Passwords Hacked (http://www.cbc.ca/news/technology/story/2012/06/06/tech-linkedin-hacked-passwords.html)

How is it possible for internet voting companies to claim their systems can't be compromised when the most secure networks in the world continue to be penetrated by hackers? Statements like these only serve to fuel hackers into proving them wrong. It is not a question of if an internet voting system will get hacked; it is only a question of when. Can the public really trust a private for-profit company to openly admit they have been hacked during an actual election? Given the financial repercussions of confirming such a penetration, it is highly unlikely any internet or electronic voting company would ever do this.

Whenever pilots are being conducted, internet voting companies do not allow the public to openly hack their systems and make any security companies sign non-disclosure agreements prior to performing any security tests on their systems. This essentially gags security companies from reporting publicly about any intrusions or vulnerabilities they detect. If internet voting systems are really the most secure then it should be mandated they allow a public open attack on their election system to prove it to the citizens.

Computer science experts around the world are speaking out against the use of online voting and in some cases have proven how vulnerable electronic voting can be. Alex Halderman, associate professor for the University of Michigan, is well versed on the dangers related to electronic voting systems and internet voting. He has demonstrated numerous times how electronic voting machines can be hacked and gained notoriety when he and his team successfully hacked the proposed Washington D.C. internet voting system in less than 36 hours. [13] While he was able to employ a number of known exploits to compromise the security of the system, in the end it came down to a single pair of quotation marks, erroneously coded into the program, which gave him full control over the system.

The FBI[14], CSIS[15], and other global intelligence agencies around the world are continuously reporting about the growing trend of cyber threats. Viruses like Red October, Flame[16], Stuxnet[17], Conflicker[18], Zues[19], and DNSChanger[20] are being detected in the wild and growing in their sophistication. In the case of Red October,

[9] National Post, December 7, 2011 – Facebook Fixes Photo Privacy Bug After Founder Mark Zuckerberg Has Account Hacked (http://news.nationalpost.com/2011/12/07/facebook-fixes-photo-privacy-bug-after-founder-mark-zuckerberg-has-account-hacked/)

[10] Business Insider, July 14, 2011 – Pentagon Admits 24,000 Files Were Hacked, Declares Cyberspace A Theater Of War (http://www.businessinsider.com/pentagon-admits-24000-files-were-hacked-declares-cyberspace-a-theater-of-war-2011-7)

[11] The Telegraph, February 11, 2012 – CIA Website Hacked In Attack 'Claimed' By Shadowy Cyber Group Anonymous (http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9076314/CIA-website-hacked-in-attack-claimed-by-shadowy-cyber-group-Anonymous.html)

[12] CBC News, February 16, 2011 – Foreign Hackers Attack Canadian Government (http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html)

[13] Scott Wolchock, Eric Wustrow, Dawn Isabel, J. Alex Halderman, February 2012 – Attacking The Washington D.C. Internet Voting System (https://jhalderm.com/pub/papers/dcvoting-fc12.pdf)

[14] CBS News, February 2, 2012 – FBI: Cyber Threat Might Surpass Terror Threat (http://www.cbsnews.com/8301-3460_162-57370682/fbi-cyber-threat-might-surpass-terror-threat/)

[15] CSIS, February 9, 2012 – Information Security Threats (http://www.csis-scrs.gc.ca/prrts/nfrmtn/index-eng.asp)

[16] Wikipedia, No Date – Flame (malware) (http://en.wikipedia.org/wiki/Flame_(malware))

[17] Wikipedia, No Date – Stuxnet (http://en.wikipedia.org/wiki/Stuxnet)

[18] Wikipedia, No Date – Conflicker (http://en.wikipedia.org/wiki/Conflicker)

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

[20] Wikipedia, No Date – DNSChanger (http://en.wikipedia.org/wiki/DNSChanger)

another intelligence gathering virus, expert estimate the virus has been operating without being detected for over 5 years.[21]

Ensure that the process is subject to adequate audit verification

Auditing the results of an election is impossible when using any online or electronic voting system. When a digital ballot is cast there is no paper trail left behind to verify the vote, so auditors can only verify the numbers produced by the internet voting system. Scytl's online election software can only produce a spreadsheet which details the candidate choice for each ballot received. There is no evidence to prove the voting system received the ballot exactly as it was cast, or didn't make a mistake during tabulation. Such was the case in Penang, Malaysia during a recent election using an internet voting system where the results were erroneously tabulated and reported.[22]

Furthermore, no recount is possible because there is no other means of recounting the ballots. The data produced by the election system is the only information generated so once again blind trust must be placed with a private for-profit company. Should any candidate choose to challenge the results of the election they will have a difficult road ahead as they do not have any means to independently verify the results. The only means to verify the election will be for each registered voter to keep a paper copy of their ballot and compare results of the digital election to the paper records. This process completely negates the purpose of using an electronic voting system.

Identify measures to be taken to promote transparency and reliability, including the use of communication or education programs to make voters familiar with the process and safeguards, or through the use of audit procedures and publication of audit results

As you can see by the previous points, electronic voting does not promote transparency or reliability. In a paper ballot election, ballots are cast and then counted in front of election officials and witnesses. Should it be necessary, an independent organization can verify the results of the election by recounting the paper ballots.

Holding elections online also opens up the possibility for the virtual ballot box to be stuffed with virtual ballots. Since the number of registered voters rarely equals the number of actual voters, internet voting provides a way for the ballot box to be stuffed with ballots from registered voters who did not participate in the election.

At no time during an electronic election does the voter have any proof that their ballot was received exactly as it was cast. The very nature of computers means votes can easily be switched for a specific candidate by either a software glitch or malicious intent. Such was the case with one electronic voting machine in Pennsylvania in

[21] Securelist, January 14, 2013 – The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic And Government Agencies (http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies)

[22] Free Malaysia Today, January 5, 2013 – DAP: Election Fiasco An Embarrassment (http://www.freemalaysiatoday.com/category/nation/2013/01/05/dap-election-fiasco-an-embarrassment/)

the U.S. Presidential Election where a voting machine was filmed switching a vote.[23] This is not an isolated occurrence as Alex Halderman has proven numerous security vulnerabilities in a number of electronic voting machines such as the Diebold AccuVote-TS[24] and the Electronic Voting Machines (EVMs) used in India.[25]

Closing Remarks

As more evidence comes out showing the growing number of security risks associated with electronic voting, internet voting, and electronic tabulation, municipalities and governments around the world are moving away from using this technology.

- In December 2012, Kitchener, Ontario rejected using online voting due to security issues and the additional costs associated with building, maintaining, and securing a database of registered voters[26]
- In May of 2011, the B.C. government rejected a proposal to allow internet voting for Vancouver's municipal election citing "a number of serious risks" related to security[27]
- In 2004, the Pentagon rejected the use of internet voting for overseas military personnel due to "fundamental security problems that leave it vulnerable to a variety of well-known cyberattacks"[28]
- and the U.S. federal government does not allow internet voting because they are concerned about the risks related to malware and fraud[29]
- The Netherlands[30], Germany[31], Ireland[32] and many other countries have also not only disallowed internet voting, but removed electronic voting and tabulation machines due to security and constitutional concerns.

Many proponents of internet voting will try to argue that internet voting dramatically increases voter participation, but as the statistics in the Staff Report from the City of Kitchner detail this is simply not the

[23] Huffington Post, November 6, 2012 – Pennsylvania Voting Machine Switches Vote From Barack Obama To Mitt Romney (http://www.huffingtonpost.com/2012/11/06/pennsylvania-voting-machine-switches-vote-obama-romney_n_2083015.html)

[24] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, August 2007 – Security Analysis Of The Deibold AccuVote-TS Voting Machine (https://jhalderm.com/pub/papers/ts-evt07.pdf)

[25] Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhumuri, Vasavya Yagati, and Rop Gonggrijp, October 2010 – Security Analysis Of India's Electronic Voting Machines (https://jhalderm.com/pub/papers/evm-ccs10.pdf)

[26] The Record, December 10, 2012 – Kitchner Rejects Internet Voting (http://www.therecord.com/news/local/article/851707--kitchener-rejects-internet-voting)

[27] Straight.com, May 27, 2011 – B.C. Government Rejects Online Voting In Vancouver Fall Election (http://www.straight.com/news/bc-government-rejects-online-voting-vancouver-fall-election)

[28] The New York Times, February 6, 2004 – Online Voting Canceled For Americans Overseas (http://www.nytimes.com/2004/02/06/politics/campaign/06VOTE.html)

[29] USA.gov, November 5, 2012 – Can You Vote Online? (blog post) (http://blog.usa.gov/post/35067724772/can-you-vote-online)

[30] ComputerWorld, May 19, 2008 – Dutch Government Bans Electronic Voting (http://news.idg.no/cw/art.cfm?id=003AE63C-17A4-0F78-31DDDC0DCFA62609)

[31] Deutche Welle, March 3, 2009 – German Court Rules E-Voting Unconstitutional (http://www.dw.de/german-court-rules-e-voting-unconstitutional/a-4069101-1)

[32] Irish Times, June 29, 2012 – E-Voting Machines To Be Scrapped (http://www.irishtimes.com/newspaper/breaking/2012/0629/breaking2.html)

case.[33] Proponents and supporters argue that internet voting is secure because people bank, shop, and file taxes online. However, these are not factual arguments proving the safety of electronic elections and numerous papers have been written to show how the two online systems are entirely different.[34] Online transactions such as these require both parties to be fully aware of the other's identity, while a voter's identity must remain completely secret from their vote. Would any of these supporters still want to do any of these activities if their identity needed to remain secret? It seems doubtful as trust would become the paramount concern.

I would like to thank you for taking this matter into consideration and I do realize that I have provided you with a wealth of information. I implore you to thoroughly research the information so you may make an informed decision. I am confident if you review all of the articles and reports listed in the footnotes you will have all the evidence necessary to put a stop to internet and electronic voting in Alberta.

Democracy demands transparency not trust, and we need to be able to trust the vote.

Respectfully,

Chris Cates

[33] 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)

[34] David Jefferson, Verified Voting, No Date – If I Can Shop And Bank Online, Why Can't I Vote Online? (https://www.verifiedvoting.org/resources/internet-voting/vote-online/)

From: David Fishback
Sent: July 9, 2013 9:20 PM
To: Clerks
Subject: Internet voting

Internet voting, if done correctly, is a good thing. It is another choice for the voters to use. I do not see any real issues with it. People use Internet for banking and now you can only use the Internet to sent your tax returns. In my professional opinion, the Internet is a great medium.

This will be an eventuality in the near future, just like processing your tax return. Guelph should be on the leading edge of this so that we can have a say in how Internet voting goes forward.

David Fishback

Subject: Municipal Election Process in Guelph

I'm sure that this is not the only reason for declining voter turnout during our city elections but I like to think that one big reason for the decline is the 'beeping ballots fiasco' of the past few elections. The use of 'beeping ballots' is simply another example of how the people who run this city have fallen victim to a slick sales pitch without putting a lot of thought into their decision.

I know what the pro-sayers of 'beeping ballots' would probably say. Technically in legal blah blah blah terms such a ballot is still 'secret' since the choice of the voter is not revealed. Is unintentionally making an error or intentionally spoiling a ballot not a choice? Why should this be revealed to the public? Even if people can prove in court that technically the voter's right to a secret ballot is still protected, 'beeping ballots' are still an arrogant infringement on that right. Would you accept condolences at a funeral from someone who was snotty and had a smirk on their face? If you want people to vote it's not only about what is legally correct. It's more about how people perceive the process.

Of course pro-sayers would also say that 'beeping ballots' eliminate the mild civil disobedience of intentionally 'spoiling a ballot'. It makes the tabulation process more efficient since we no longer need to deal with 'spoiled ballots'. Let's look a little bit at the notion of 'spoiling a ballot'. I don't mind revealing that during an election many years ago I intentionally spoiled my ballot. I placed a large X over the entire paper ballot with my pencil and placed it in the box. I wanted to send the message that yes I am very much interested in the voting process but I felt that all of the possible candidates sucked and none deserved my vote. If I revealed this during some kind of election poll I'm sure the polster would be very interested in this information. Its another piece of valuable data that helps to reveal what is truly on the mind of voters. We live in a bare-bones minamalist democracy as it is. Once every four years thereabouts we get to cast one paltry stinking vote for each of three elections for three levels of government. And if we're really lucky we may get to vote in a referendum once every other blue moon. I would think that when the opportunity does present itself we should be interested in collecting as much useful data from the process as possible.

Now the pro-sayers may also say 'Oh but spoiled paper ballots can be nasty'. People can write nasty words during the process of 'spoiling their ballot'. OMG a vote counter has just been assaulted by annonymous words on paper. Who cares??? We've all seen writing on bathroom walls, grafitti on walls and the like. I'm sure we're all stronger people because of it. Let people have their say!

But after all is said and done I'm not actually against eliminating the 'spoiling of ballots'. I think its a really stupid idea but if the powers that be really have their heart set on it so be it. However it needs to be done properly. Any warning of error needs to be done in secret during the voting process. Or using technology you can physically prevent someone from spoiling their ballot. I've been an IT programmer for 25 years so I know all about forcing data integrity in computer apps using radio button, comboboxes and so on. There could also be a 'None of the above' option on all ballots. Oh, but the pro-sayers might say that this would discourage voting for a candidate. But really if someone doesn't like any of the candidates do you really think you are going to get a legitimate vote from that person anyway? I don't think so.

I want a voting process that I can see is fair and honourable and respects all of my rights as a voter. To me that is the Canadian way. Personally if I see one more public beeping ballot during any election I will promptly turn around, leave and never vote in another election ever again.

I implore you, NO MORE BEEPING BALLOTS!!!!

Sincerely,
Sonny A. Sorensen

Dear Members of the Governance Committee,

I hope this finds you well. I am writing regarding the proposal for Internet Voting for the Guelph 2014 municipal election.

In everything that I have had read, this is not being implemented as a cost saving initiative but rather to increase voter turn out. I was happy to know that the report has included the many concerns such as security, transparency and cost associated with internet voting. I personally believe that having both voting options are important to increase voter turnout. However, I also believe that are there are a few important things that internet voting does not address or manifest.

I have worked a variety of positions in every municipal, provincial and federal election for the past 35years. Thus, I have gained a great insight into electors and election day.

One thing that stands out is that there is are several generations who not only believes that it is their right but their duty to vote. Those in their 70's and up tend not to miss a vote. While many of these generations are very competent with technology, there are just as many who are not. Therefore, in my opinion, it very important that Guelph must provide physical voting stations, with accessible parking, including in our many adult lifestyle and retirement homes.

At the same time there are many new and young voters for whom computer technology is an integral part of their lives. So on line voting would be an logical extension of their lifestyle.

The other group of voters that many people do not realize make up a large portion of our voters are those who are lesser advantaged and those with physical disabilities. Therefore, it is imperative that we have physical voting stations and computer access available for these populations. Also that on-line voting options in public places have appropriate technology applications available for those with sight or other physical challenges (ie: a stroke survivor).

There is a wonderful "buzz" and community created when people go out to physical polling stations on Election day. We are long past meeting one another and chatting about politics while looking for our names on the registration list posted on a telephone poll. Many still enjoy getting out to vote and being a part of the day. I am always as excited as someone who announces they have been waiting for this day, their first vote.

We build community when setting up physical polling stations in locations such as Fire Halls, libraries Spiritual sites and schools. Teachers bring children in to watch the elector system at work first hand. We increase our understanding of accessibility when we ensure that a site can be entered and navigated easily by someone using a mobility scooter. Polling signs throughout the city remind busy people that it is voting day. We get to know our neighbours.

Thus, I believe that if the goal is to increase voter turn out. We must provide a suitable combination of options to cast our vote. I hope to see some of you at the polls.

Take Care
Barbara Mann