Correspondence – Susan Watson

Cameron Shelley

Guelph

April 18, 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