Chris Cates
111 Royal Terrace
Edmonton, AB T6J 4R2

March 15, 2017

Elected representative,

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

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

Increased Turnout

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

Costs Less

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

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

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

Upholding Democratic Principles

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

These core principles are:

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

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

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

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

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

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

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

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

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

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

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

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

Security of the voting system cannot be ensured

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

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

---

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

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

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

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

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

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

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

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

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

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

[19] TechCrunch, April 7, 2014 – Massive Security Bug In OpenSSL Could Affect A Huge Chunk Of The Internet (http://techcrunch.com/2014/04/07/massive-security-bug-in-openssl-could-effect-a-huge-chunk-of-the-internet/)
[20] CBC News, April 9, 2014 – Heartbleed Bug May Shutdown Revenue Canada Website Until Weekend (http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742)
[21] J. Alex Halderman, November 2014 – Security Analysis of the Estonian Internet Voting system (https://jhalderm.com/pub/papers/ivoting-ccs14.pdf)
[22] Vanessa Teague, April 2015 – The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election (https://arxiv.org/pdf/1504.05646v2.pdf)
[23] J. Alex Halderman, June 2012 – Attacking the Washington, D.C. Internet Voting System (https://jhalderm.com/pub/papers/dcvoting-fc12.pdf)
[24] Aleksander Essex, December 2016 – The Cloudier Side of Cryptographic End-to-End Verifiable Voting: A Security Analysis of Helios (https://whisperlab.org/helios/helios.pdf)
[25] FireEye, March 2017, M-Trends 2017 (https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html)
[26] Mozilla, March 2017 – Hackers, Trackers and Snoops: Our Privacy Survey Results (https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5#.a5c2a0apb)

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

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

> ***"The security risks associated with Internet voting pose a serious threat to a number of these principles. The Clerk is committed to exploring technological and other solutions that improve voting accessibility but remains of the opinion that current Internet voting systems are not secure enough for large scale use in binding, public elections."***[27]
> City Clerk, Toronto, Ontario, Executive Committee Report for Action
>
> ***"Do not implement universal Internet voting for either local government or provincial government elections at this time."***
> ***"The risks of implementing Internet voting in British Columbia outweigh the benefits at this time."*** [28]
> *Independent Panel on Internet Voting Recommendations Report to the Legislative Assembly of British Columbia*
>
> ***"I still think the in-person voting is the most secure and safe way of voting."*** [29]
> Gary McLeod, P.E.I. Chief Electoral Officer
>
> ***"Should we start using Helios for public-office elections? Maybe US President 2016?***
> ***No, you should not. Online elections are appropriate when one does not expect a large attempt at defrauding or coercing voters. For some elections, notably US Federal and State elections, the stakes are too high, and we recommend against capturing votes over the Internet. This has nothing to do with Helios itself: we just don't trust that people's home computers are secure enough to withstand significant attacks."*** [30]
> *Internet Voting Maker, Helios Voting*
>
> ***"Internet voting may well remain a good idea for private elections, for EBAs, and for popular events but it will never have the qualities needed for high stakes public elections even party elections with outcomes affecting the general public."***[31]
> Craig Burton, founder of online voting maker, Everyone Counts

---

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

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

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

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

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

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

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

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

Conclusion

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

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

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

Respectfully,

Chris Cates

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

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