InternetNZ

InternetNZ

Exposure draft Local Electoral (Online Voting Trial) Amendment Regulations 2019

InternetNZ Submission

12 November 2018

InternetNZ

Table of Contents

1. Introduction

1.1 InternetNZ welcomes the chance to submit on these draft regulations.

1.2 Trust in democratic institutions is a vital and pressing issue for the Internet era. We have engaged constructively with past processes considering online voting, offering our analysis as well as venues for informed and open conversation on the issues. We are doing our best to support consideration of the issues.

1.3 However, current work on online voting must consider the current context. In 2014, the Internet seemed beneficial or benign for democracy. In 2018, the Internet's effects on democracy have proven much more hostile.

1.4 These draft regulations are proposed under the Local Electoral Act 2001, which sets out principles including "public confidence in, and public understanding of, local electoral processes"[1]. Our submission assesses the draft regulations against this standard.

1.5 With public confidence in elections facing new challenges, we want the regulations to offer a high level of assurance. New Zealanders need to trust their voting system, and the system needs to deserve that trust.

2. Summary of Submission

2.1 This submission sets out our thoughts, concerns and recommendations in relation to:

a) the challenges to online trust in 2018

b) the security challenges from external risks

c) the security of the online voting system itself

d) ensuring the safe operation of online voting

e) our concerns with the process surrounding the exposure draft regulations.

[1] Local Electoral Act 2001, s 4(1)(c)

InternetNZ

3. Recommendations

3.1 Our collated recommendations to the Department are as follows.

Challenges to online trust in 2018

- **We recommend that a** cautious and considered approach is taken to moving important institutions, like voting, online.

Protection from external risks

- We recommend that the Regulations require a local council's CE report to not only confirm that the online voting system will meet the established criteria but also outline the security risks that cannot be mitigated.

Security of the online voting system itself

- To strengthen the assurance, we recommend a new requirement be added to R135C(2)(a). that requires elections to be free from interference.
- We recommend a deliberative public conversation, engaging the local information security community to develop a shared understanding of the avoidable and unavoidable risks of online voting.
- We recommend a sufficiently independent audit report is undertaken to offer assurance to the public that any voting system will face robust scrutiny before it is used in an election.

Ensuring the safe operation of online voting

- We recommend that you consult with a range of experts to assess current and future options for authentication of an online voting system, and the potential compromises these involve.
- We recommend that more consideration is given to double voting remedies, with a particular emphasis on remedies that will work well for overseas voters, or those with mobility and accessibility issues.
- We recommend that an independent reviewer is appointed before any online voting trial.

3.2 Detailed recommendations on specific parts of the Act and regulations are included in the body of the report.

4. Challenges to online trust in 2018

Misinformation targets voter behaviour

4.1 Social media "bots" and other automated tools are being used in deliberate campaigns to influence voter behaviour. Oxford research has highlighted 48 online influence campaigns across the globe since 2010[2].

4.2 Examining false and harmful information online, a recent report by the Council of Europe highlights "dis-information campaigns specifically designed to sow mistrust and confusion" as a threat to democracy.[3]

---

[2] Oxford Internet Institute Computational Propaganda project: https://comprop.oii.ox.ac.uk/research/cybertroops2018/

[3] Council of Europe, *Information Disorder*, p 4. https://firstdraftnews.org/coe-report/

InternetNZ

Our distance and size do not protect us online

4.3 The Internet bridges distances, for good and ill. New Zealanders are on the same platforms and can be affected by the same tools used to target and influence political conversations and voter behaviour overseas.

4.4 There are clear reasons for other countries to care about New Zealand's economic and political decisions. Beyond direct trading relationships, we have valuable marine areas, intelligence relationships, and an orbital launch facility. There is evidence that overseas powers have moved to monitor, participate in, and perhaps influence our domestic political processes. Work by Professor Anne-Marie Brady offers one case study, setting out evidence that China's government and party institutions have sought to build funding and other relationships of influence at all levels of our political system.[4] We should not be paranoid or surprised by this, but nor should we be naive.

In 2018, moving online risks losing people's trust

4.5 InternetNZ supports the Internet as a beneficial force for all New Zealanders. That also means understanding and responding to risks.

4.6 Reporting by CERTNZ shows increased reporting of online crimes and security risks affecting New Zealanders.[5] In general, putting a system online makes it easier to affect many people at once. In the current context, we think a cautious and considered approach must be taken to moving important institutions like voting online.

5. We need protection from external risks

5.1 In 2018, maintaining trust on systems connected to the Internet is difficult. Systems that people use, though they might be relatively secure on their own technical terms, can be undermined by external risks that affect their users.

5.2 One example is phishing, where attackers create fake emails and websites, that convince users to share their details or behave as the attacker wants. Phishing is the most common type of security incident reported to CERTNZ.[6]

5.3 Even if all the proposed criteria under R135C(2)(a) are satisfied, external risks of this type could undermine trust in an election, particularly an election where online voting is used. Table one, below, sets out three examples of external information security challenges and how they could affect online voting.

---

[4] Anne-Marie Brady, https://www.wilsoncenter.org/sites/default/files/for_website_magicweaponsanne-mariesbradyseptember2017.pdf

[5] CERTNZ, Quarter 2 Report 2018, https://www.cert.govt.nz/about/quarterly-report/quarter-two-report-2018/

[6] CERTNZ, Quarter 2 2018 Report

Table one: external information security challenges for online voting

Challenge	What is it?	How could it affect voting?
Phishing	Faked emails and websites persuading people to share information e.g. "A vote was recorded in your name, click here to check we got it right"	Voter login details could be collected by phishing and used to enter votes. Fake election emails could be used to undermine trust in an election, confusing voters as to which emails and websites are legitimate.
Malware on user devices	People's phones, tablets, and computers may be running malicious software that monitors or alters information	Votes could be monitored or manipulated by software running on a voter's device, or on a network used for voting before they are transmitted to the online voting system.
Denial-of-service	Computers flooding a device or service with data, making it unusable	Voter devices could be cut off from voting, even if the online voting service remains online. If this were to happen in the last 2-3 days of the voting period, voters would not be able to vote by post before ballots were counted.

5.4 New Zealand deserves a clear articulation of which of the known information security and cybercrime issues that New Zealanders face could not be mitigated while voting online and therefore need to be considered acceptable risks.

5.5 We recommend that the Regulations require a local council's CE report (R135C) to not only confirm that the online voting system will meet the criteria set out in R135C(2)(a), but what outstanding security risks **cannot be mitigated** and would need to be accepted as a risk.

6. Security of the Online Voting System

We support rigorous assessment before allowing any online system

6.1 To uphold trust in our elections, New Zealanders need a voting system that is trustworthy, and that is seen to be trustworthy. These regulations must give New Zealanders that assurance. This needs to be done by requiring a robust and independent evaluation before any online voting system can be used at an election.

6.2 To deliver this assurance, the draft regulations offer a process as follows. Before adopting an online voting method, a local authority must receive a report from its Chief Executive, accompanied by an audit report. Both reports must confirm that the voting system meets criteria set out in R135C(2)(a), enabling "a voting process that is secret, accurate, available and reliable, auditable, verifiable, secure, and accessible".

We support the R135C criteria

6.3 R135C sets out criteria which a Chief Executive's report must address to support a voting method for adoption. This report must state that the voting system will enable a voting process:[7]

a) that complies with the Act and regulations

b) that is secret, accurate, available and reliable, auditable, verifiable, secure, and accessible.

6.4 We support these criteria for assessing risks and features internal to a voting system itself. In particular, we welcome the accessibility requirement. Voting should be easier for people with limited mobility, those who are blind or have reading disabilities, and those who are overseas during the election period.

They should be expanded to require that elections be free from interference

6.5 The Local Electoral Act 2001 establishes a principle of "upholding public confidence in local elections". As set out above, there are plausible risks, external to the voting system itself, which could undermine public confidence in an election where online voting is used.

6.6 To strengthen the assurance given by R135C, we recommend a new requirement under R135C(2)(a), to address external risks of the type discussed above.

6.7 In table two we have added our proposed requirement under R135C(2)(a), so it would apply under draft provisions for audit reports and suspension of online voting.

6.8 Our primary rationale for this proposal is to address particular concerns relating to online voting systems. In principle, it would also apply to concerns with in-person voting, such as reports of large-scale vote-buying, or voter coercion. Our goal is to explicitly provide for a response to external risks, if these external risks would tend to undermine public confidence in an election.

Table Two: updated R135C(2)(a)

i	Secret	...so that data is stored in a way that prevents any person from being able to associate a vote with an elector without the elector's consent (subject to paragraphs (iv) and (v))
ii	Accurate	...so that each vote cast accurately reflects the intentions of the elector and is recorded accordingly
iii	Available and Reliable	...so that the online voting system performs as intended and so that an elector can cast their vote at times when postal voting is also available
iv	Auditable	...so that votes cast online can be reviewed and independently verified in the event of a recount or a disputed vote
v	Verifiable	...so that it is possible to verify a complete and accurate record of votes cast online

[7] R135C(2)(a)

vi	Secure	...so that the online voting system, and data held in the system, will not be subject to unauthorised access or manipulation
vii	Accessible	...so that electors with disabilities and those who are situated away from their registered address are able to vote easily and independently
vii	**Free from interference**	**...so that in context there are no security concerns or other external factors which would tend to undermine public confidence in the voting system.**

These criteria will be challenging to implement

6.9 Building a system that will satisfy the R135C(2)(a) criteria will be extremely difficult, based on conversations and comments from experts in application security.

6.10 One particular challenge is the democratic principle of a secret ballot, here represented by the secrecy requirement at 135C(2)(a)(i). In most sensitive systems, transactions can be tracked and verified by identifying the people involved. This allows for remedies such as reversing a transaction if a problem is identified. That is not possible in a well-designed system for online voting as identifying a user or device throughout the system would compromise the requirement of secrecy.

6.11 Showing that a system satisfies all these criteria, in a way that voters can understand, is even more difficult. We support a robust and independent audit process to ensure that these criteria are properly applied, and that any use of online voting deserves public confidence.

6.12 We would support a deliberative public conversation on these criteria, engaging the local information security community to develop a shared understanding of:

a) what an online voting system would need to deliver to each requirement

b) compromises or trade-offs between requirements

c) avoidable and unavoidable risks in a well-designed implementation.

A robust and independent audit report pre-election is critically important

6.13 We welcome the requirement for an audit report. To uphold public confidence in an online voting system, New Zealanders need credible assurance that, any proposed voting system will face robust scrutiny before it is used in an election. That scrutiny must be independent and draw on expertise in a range of areas.

6.14 We are concerned that the draft regulations do not require a sufficiently independent or informed audit report. As drafted, R135D requires the audit report have a single author, who must be appointed by the relevant Chief Executive.

The audit report must draw on relevant expertise

6.15 An online voting system is a technical system that serves a democratic function. To uphold public confidence, the audit report should be informed by expertise on a range of issues, including the delivery of computer systems, the proper conduct of elections, and security issues for online voting.

6.16 The current drafting does not require expertise on all these issues. Under R135D(2), the author could be someone with a qualification "relevant to current practices of project management and auditing", or someone skilled in interpreting controls on online voting systems. Either choice risks neglecting skills and information that are important to assessing an online voting system. In practice, it may be that authors are selected based on which skills are easiest to find, not based on skills needed to robustly assess a voting system.

The audit report must be independent

6.17 An audit report must have a high degree of independence, to enable an honest and robust assessment of potential risks and concerns. Current drafting provides that an author would be appointed by the Chief Executive and would make their own assessment of potential conflicts of interest. This is not a robust independence requirement.

The audit report must consider potential risks and plans to mitigate these

6.18 To serve its purpose, an audit report must consider plausible risks to an online voting system, and options for mitigating those risks.

We recommend requiring a more robust audit report

6.19 We recommend changes to R135D, to require that an audit report is informed, independent, and considers risks.

6.20 We recommend a requirement that the audit report draws on expertise in each of the key subject areas. Those areas may include:

a) Technical and security considerations for an online voting system

b) The conduct of local elections in New Zealand

c) Project management and delivery relevant to an online voting system.

6.21 We recommend a requirement that the audit report:

a) offers an independent assessment of the voting system

b) is produced by people who are independent from the Chief Executive, and who have no direct interest in the outcome of the reporting process.

6.22 We recommend that R135E is modified to ensure that the audit report consider and report:

a) on risks to the voting system under the R135(2)(a) criteria

b) offer and assess options for mitigating identified risks.

7. Online voting must operate safely

Authentication must be accurate, reliable, and easy

7.1 We welcome the provision of proposed options to check the identity of an elector, in preparation for an online voting option. Authentication is a difficult challenge, as it must offer reasonable security, but also be easy to use by voters.

7.2 Authentication must adequately address security risks, from interference with individual electors, to broad-scale attempts to influence an election. To deserve the confidence of New Zealanders, we should be aiming for better security than postal voting.

All proposed options require difficult compromises

7.3 Designing a system for accurate, secure authentication is difficult. Making it easy to use is more difficult. Doing so while preserving the secrecy of the ballot is an extremely demanding technical challenge.

7.4 We are not persuaded that any of the proposed authentication options can adequately deliver both security, and ease-of-use.

A - Access code and date of birth

7.5 Option A relies on a paper ballot as one mode, combined with a date of birth and the electoral roll as a second mode. This option creates a substantial risk of voter impersonation, which may be by close contacts, or by unknown people online.

7.6 Dates of birth for many people will be easily identified by close contacts, or by people with access to social media or other records.

7.7 We do not support this option.

B - Active registration (or pre-registration)

7.8 This option requires an active step to register as an online voter. The extra steps in authentication make this option relatively less convenient. They also create potential risks to a voter's privacy and security.

7.9 Registration requires provision of a name and address, as well as verification. Verification may be by providing a driver licence number, a passport number, or by RealMe. On verification a voter is asked to provide a mobile phone number or email address.

7.10 RealMe is not popular enough to offer a useful verification method. For other methods, the requirement to share valuable ID and contact information raises the privacy risks of online voting, putting more information at risk of being shared in the event of a breach.

7.11 There is limited protection against impersonation by close contacts. A voter's close contacts are likely to have physical access to their ID numbers.

7.12 Finally, the sorts of information being used for authentication would offer a valuable target for phishing campaigns. Scammers could send fake emails, similar to those used for voter registration, obtaining valuable contact and ID information from real people, for use or for sale to other criminals.

C - Authentication code

7.13 Option C provides for a code to be sent to each elector around the time voting papers are issued. This can be by postal or other means.

7.14 Relying on postage reduces the benefits of online voting for accessibility and cost. Electors must receive two different mail deliveries to vote.

7.15 For another contact method to be used, that contact information must be gathered and held by electoral officers, raising many of the same privacy and phishing concerns as Option B.

Consult with experts on authentication options

7.16 The proposed authentication options fall short of what is needed to assure public confidence in the integrity of an election where online voting is used.

7.17 We recommend that you consult with a range of experts to assess current and future options for authentication, and the potential compromises these involve.

We need better remedies for double-voting

7.18 The Local Electoral Act 2001 allows only one vote to be recorded per elector.[8]

7.19 Even with an effective online voting awareness campaign, we can expect that many voters will submit both postal and online votes. Many people will find it confusing or unfamiliar to have a new option for voting. Some of these double-votes may express different intentions. There is also a risk that malicious actors will obtain voter credentials, or otherwise use security weaknesses to register a vote for other electors.

7.20 We understand that there are two proposed remedies to double-voting. As set out below, we are doubtful that, in practice, these remedies will restore public confidence if there is confusion about double-voting.

7.21 The first remedy is R135J, which allows for a voter to verify an online vote in-person. This is unlikely to be taken up by voters who are confused, or where someone else takes their identity to register a vote. Many of these people will simply not know that an online vote has been registered in their name. If there is widespread concern, the option to verify in-person is unlikely to work well at scale.

7.22 The second remedy is the option of recording a special vote. We understand that a special vote would override either an online or a postal vote. This has the same problems as the above remedy. Electors needing a special vote to overcome confusion are least likely to be aware of the option, and it cannot scale to widespread demand.

7.23 None of these remedies will work well for overseas voters, or those with mobility and accessibility issues.

Suspension of voting and external risks

7.24 We have proposed an external risks requirement under R135C(2)(a), to allow for responses to external events which may undermine public confidence. These include, for example, phishing emails seeking to collect authentication details or to influence voter behaviour.

7.25 R135M allows for suspension of online voting in the event of a failure or breach. Our proposed change to R135C(2)(a) that calls for elections to be free from interference will ensure online voting can be suspended if interference occurs that undermines public confidence in the voting system.

Close of voting period

7.26 For electors who have already commenced online voting, R135I provides for a 5-minute extension beyond noon, with notifications at noon and at 12:04.

7.27 Notifying an elector that they have 5 minutes to complete voting, then 1 minute, does not seem helpful, particularly in terms of the accessibility criterion under R135C(2)(a)(vii). For electors who can read a conventional screen, a continual countdown to noon on polling day may work better.

7.28 If notifications are proposed for accessibility reasons, then more than 5 minutes is likely to be required. Given the complexity of local elections and the large number of candidates and ballots to be cast, registering a

[8] Local Electoral Act 2001, s 20.

meaningful vote may take more than 5 minutes even for electors using a conventional screen and input methods.

7.29 We would like to see evidence that requirements with accessibility implications, including this one, are informed by consulting experts in user experience and accessibility.

We welcome data security requirements

7.30 We support the provision of security requirements limiting the use and retention of information collected for online voting.

7.31 The electronic collection, use, and deletion of records creates some unique security and privacy risks. In our view, election officers should have access to technical expertise to ensure that their treatment of records maintains the privacy of voters, and the security of their systems.

Post-election review and audit

7.32 These draft regulations are intended to enable a trial of online voting. If any trial takes place, there should be provision for a full and independent review, considering not only the process and effects within each local authority, but the broader lessons and context, across New Zealand, of a trial of online voting.

7.33 The review requirement in R135S is a report by each electoral officer to the relevant local authority. This is not an adequate review requirement. It is difficult to understand how the lessons of online voting will be learnt without a much more comprehensive review of the whole trial of online voting across the different councils that take part.

7.34 We recommend that the regulations require the Department to appoint an independent reviewer of the trial of online voting. This independent reviewer could be from the Electoral Commission, or from a competent international body. Any review would need the expert support required to evaluate technical aspects of any trial.

7.35 Without a commitment to overall monitoring and review, we cannot see how a trial of online voting is justified. We think such a review should be a condition of any trial proceeding.

8. Process and other comments

8.1 Changes to the voting system deserve the highest possible level of consultation and democratic deliberation. Our voting system is how New Zealanders empower, direct, and hold to account our government institutions. A potential move to allow online voting combines those democratic sensitivities, with the changing and complicated world of developing technology.

8.2 The proposal is not just a trial. These draft regulations could change the immediate outcomes of real elections. The changes should therefore be considered as a substantive regulatory change.

8.3 In that context, we are concerned that vital due process is losing out to speed. These are complex issues, which deserve time, consideration, and wide consultation. The goal of enabling a trial next year, with the required business, technical, and legal tools in place, is competing with the space needed to adequately address these issues.

8.4 The Government has an expectation for good regulatory stewardship that agencies provide robust analysis and advice to Ministers before decisions are taken on regulatory change. Despite that expectation, this process has not

included a regulatory impact assessment, though it addresses a change with democratic implications, and perhaps long-term consequences for New Zealanders' trust in our political system.

8.5 The Department, as a regulatory agency, is required to undertaking systematic impact and risk analysis, including assessing alternative legislative and non-legislative policy options. We have requested, but not seen, evidence that this has been undertaken.

8.6 The *Government Expectation for Good Regulatory Practice* outlines a clear expectation that government regulatory agencies give appropriate effect to good regulation principles and regulatory stewardship responsibilities. This includes undertaking policy in an open and transparent manner.

8.7 Policy work of this kind requires open and transparent work, including adequate consultation. The short timeframe for reviewing the regulations is compounded by the lack of a discussion document to explain what the draft regulations are trying to achieve. We, and others, are commenting on the how, without a full understanding of the why.

8.8 We are not convinced that the clear consultation requirement under s139 of the Act has been satisfied by the process to date. InternetNZ is a motivated and visible participant in this conversation. Despite that, we were given only a limited window to engage with our community and respond to the draft regulations. We are aware of other interested and expert people, who have not been able to submit in the available time.

9. Want more detail? Get in touch!

9.1 Thank you for taking the time to review our submission.

9.2 Despite our concerns about the process followed, we have engaged with the regulations, and the policy intent behind them, as best we can, seeking to provide you with useful and practical recommendations to improve the regulations.

9.3 However, current work on online voting must consider the current context. In 2014, the Internet seemed beneficial or benign for democracy. In 2018, the Internet's effects on democracy have proven much more hostile.

9.4 As we have stated at the beginning of our submission, trust in democratic institutions is a vital. We believe this process will have fundamental implications for our democratic process, and the potential long-term consequences for New Zealanders' trust in our political system. As such, we encourage you to take a cautious and considered approach to moving important institutions, like voting, online.

9.5 If you have any questions or would like to meet with InternetNZ to discuss this submission please contact Ben Creet, Policy Manager (ben@internetnz.net.nz; 021 246 3228).

Ben Creet

Policy Manager