Submission to the Inquiry into the Electoral Legislation Amendment (Miscellaneous Measures) Bill 2020

July 3, 2020

Dr Michelle Blom[1]
School of Computing and Information Systems
University of Melbourne
[redacted]

Prof Rajeev Goré
Research School of Computer Science
Australian National University
[redacted]

Prof Philip B. Stark[2]
Associate Dean of Mathematical and Physical Sciences
University of California, Berkeley
[redacted]

Prof Peter Stuckey
Monash University
[redacted]

A/Prof Vanessa Teague[3]
Thinking Cybersecurity and the Australian National University (Adj.)
[redacted]

Dr Damjan Vukcevic
School of Mathematics and Statistics
University of Melbourne
[redacted]

[1]Michelle Blom is a member of the Australian Greens.
[2]Philip B. Stark serves on the Board of Advisors of the U.S. Election Administration Commission
[3]Vanessa Teague is an advisory board member of Verified Voting, a non-governmental US organization working toward accuracy, integrity and verifiability of elections.

We are a team of computer scientists and statisticians with a longstanding research interest in election security. This submission reiterates many of our previous recommendations for improving the conduct of the electronic aspects of Australian elections.

1 Introduction

If electronic voting or counting are conducted without adequate attention to transparency, privacy or verification, this can expose our elections to undetectable fraud. The bill should be amended to better protect the privacy and integrity of Australian elections.

1. The currently vague clause about allowing ballot marking with "other technologies" should specify that the vote is marked on a paper ballot in a way that allows sighted voters to verify that their vote matches their intention.

2. If electronically assisted voting is to be introduced in polling places, it should include a voter-verifiable paper record to allow sighted voters to verify directly that their vote matches their intention. On-screen or audio "verification" is utterly meaningless. Voters who are able to mark a ballot by hand should be encouraged to do so. No voter should be required to use electronic technology to mark a ballot.

3. The Senate count should be required to have a transparent, public audit of the paper ballots against the electronic preferences. This should be conducted in a way that allows Scrutineers to check both the algorithms and the data.

4. It should be recognised that no remote voting system exists that allows Antarctic voters any real vote privacy or option to verify their votes.

2 Methods for marking a ballot paper

The bill's current wording, that voters are provided with "an implement or method for voters to mark their ballot papers" seems clear enough, but we have seen in other jurisdictions that the term "ballot paper" is deliberately misinterpreted to mean an electronic record without a paper backup. This exposes the vote to large-scale manipulation and fraud. Hence we suggest that, for the avoidance of doubt, a clause is added that specifies that the vote should be recorded on paper, in a way that allows the voter to verify directly that it has been recorded according to their intention. For instance, encoding the vote in a barcode or QR code is not acceptable: the official vote should be human-readable. To protect the privacy of voters who mark ballots using electronic technology, those ballots should be designed to be difficult to distinguish from hand-marked ballots.

Recommendation 1. ***[75 Section 206]*** *after "must have an implement or method for voters to mark their ballot papers," insert, "The method must provide every voter the opportunity and means to verify directly that their vote has been correctly recorded on a paper ballot."*

3 Electronically assisted voting for voters with disabilities

Australia's existing electoral law provides for electronically assisted voting in polling places for voters whose disabilities make it difficult or impossible for them to mark a paper ballot by hand. Our

understanding of the bill is that it shifts this provision from an option that the AEC may implement, to an obligation that it must implement, without otherwise changing the provision.

We support the provision of electronically assisted voting in a polling place for voters whose visual or dexterity impairments make it difficult or impossible to mark a paper ballot by hand. However, neither the existing legislation nor the bill adequately protects the integrity or privacy of the vote. It is not advancing the democratic rights of voters with disabilities if their only technological option exposes their vote to privacy breach and fraud. Fortunately, the simple solution matches our recommendation for every other voter: ensure that the method gives every voter a way of verifying that their vote has been recorded on a paper ballot in a way that matches their intention. We recognise that this does not directly help voters who are completely blind, though there are assistive technologies that can help them to verify an appropriately designed paper ballot.

Recommendation 2. ***[66 Subsection 202AB(1)]*** *after "an electronically assisted voting method to be used by sight-impaired people to vote," insert, "The method must provide every voter the opportunity and means to verify that their vote has been correctly recorded on a paper ballot."*

If the Bill is intended to force the AEC to implement a method of Internet voting, then this is highly inadvisable: every Internet voting system that has received genuine independent assessment has been found to have serious vulnerabilities facilitating privacy breach or electoral fraud [9, 7, 4, 5]. For example, the NSW iVote system has had serious security, privacy or reliability problems every time it has run in a state election[4] [6, 3, 8].

We remind the committee of our recommendation to the Inquiry into the 2019 election:

Recommendation 3. *Do not allow Internet voting, email voting, web-loading PDFs or any other form of remote paperless e-voting.*

4 Auditing the Senate count

The non-transparent nature of the Senate scanning and counting process has always been a serious concern. The absence of rigorous auditing of the paper records means that accidental errors or deliberate manipulation might go undetected, particularly for preferences other than "1" since they are entirely dependent on the electronic process. This concern has particular urgency this year, because Scytl, the foreign company that provided the "Senate Counting Solution"[5] has recently gone in to liquidation, reportedly with debts of about 80 million Euros. Whoever produces or updates the software for the Senate counting solution could potentially introduce bugs or deliberate security flaws to allow themselves or others to manipulate the results.

Our recent results [1] show that even random errors can introduce political biases.

Rigorous election audits are commonplace in the USA—we have successfully conducted a pilot risk-limiting audit of preferential elections for the San Francisco local government elections. Although we do yet not have a risk-limiting method for completely auditing a Senate election, there are some reasonable approaches [2]. A thorough statistical audit of some aspects of the election would be a huge improvement to the transparency and integrity of the process.

It is urgent to mandate a full, open, transparent audit of the Senate ballot papers against the electronic preference data, so that the AEC and every other Australian can have confidence that the elected Senators accurately represent the choice of the people.

This increases the urgency of our recommendation to the Inquiry into the 2019 election:

[4] https://www.itnews.com.au/news/nsw-ivote-registration-goes-down-on-election-eve-522842
[5] `https://www.tenders.gov.au/Cn/Show/471f2731-fa2f-e235-5e5d-91fb7b9a53c1`

Recommendation 4. *When the preference data files for Senate votes are published, there should be a rigorous statistical audit to check that they accurately reflect the paper ballots. This should be conducted in a way that allows Scrutineers to check both the algorithms and the data.*

5 Antarctic voters

We do not understand the purpose of the following part of the bill:

> **67 After subsection 202AB(1)** Insert:
> (1A) The regulations must provide for an electronically assisted voting method to be used by Antarctic electors to vote at general elections, Senate elections and by-elections.

The explanatory memorandum's explanation, that it will "expand the electronically assisted voting methods available for sight impaired persons, to Antarctic electors," makes little sense: filling out a paper ballot remotely is not verifiable. Furthermore, there are privacy concerns (as there are for sight-impaired voters) if the person's vote is conveyed over a network without rigorous security requirements.

We understand that this has been described to Parliament as facilitating phone-assisted voting, but neither the legislation nor the Bill actually specifies this explicitly. We are unable to find any mention of phone voting in the Electoral Act or the Bill, nor any relevant technical information or security standards anywhere. The legislation should be unambiguous and should contain clear, mandatory standards for privacy, verifiability and security.

Recommendation 5. *Reconsider the sections relating to Antarctic voters. If specific voting methods were intended, then make these explicit, while also mandating clear standards for privacy, verifiability, and security. Otherwise, remove these sections.*

References

[1] Michelle Blom, Andrew Conway, Vanessa Teague, and Damjan Vukcevic. Random errors are not politically neutral. arXiv, 2020. Available at `https://arxiv.org/abs/2007.00854`.

[2] Berj Chilingirian, Zara Perumal, Ronald L. Rivest, Grahame Bowland, Andrew Conway, Philip B. Stark, Michelle L. Blom, Chris Culnane, and Vanessa Teague. Auditing Australian Senate Ballots. arXiv, 2016. Available at `http://arxiv.org/abs/1610.00127`.

[3] Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague. Trust implications of ddos protection in online elections. In International Joint Conference on Electronic Voting, pages 127–145. Springer, 2017.

[4] Pierrick Gaudry. Breaking the encryption scheme of the Moscow internet voting system, Aug 2019. Available at `https://members.loria.fr/PGaudry/moscow/`.

[5] T Haines, SJ Lewis, O Pereira, and V Teague. How not to prove your election outcome. In 2020 IEEE Symposium on Security and Privacy (SP), pages 1042–1058, Los Alamitos, CA, USA, May 2020. IEEE Computer Society.

[6] J Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In International conference on e-voting and identity, pages 35–53. Springer, 2015.

[7] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J Alex Halderman. Security analysis of the estonian internet voting system. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages 703–715. ACM, 2014.

[8] Vanessa Teague. Faking an ivote decryption proof: Why the decryption proof flaw identified in the swisspost system affects the ivote system too, Nov 2019. Available at `https://www.thinkingcybersecurity.com/iVoteDecryptionProofCheat.pdf`.

[9] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J Alex Halderman. Attacking the washington, dc internet voting system. In International Conference on Financial Cryptography and Data Security, pages 114–128. Springer, 2012.