Answers to Questions on Notice

A/Prof. Vanessa Teague
Thinking Cybersecurity
and the ANU
she/her pronouns
[redacted]

May 31, 2021

This is a partial answer to the question of how ACT legislation should change to better demonstrate the integrity and correctness of election results.

I agree entirely with the answers given by T Wilson-Brown in their email of 31st May 2021—my answer addresses different aspects on the understanding that I otherwise echo T's answers.

I particularly agree with T that this needs to be an ongoing discussion between technical experts and the committee, the legislative assembly, voters, candidates, and Elections ACT. We can advise on which technical solutions have what security and privacy properties, and on which ideas for legislative change would probably incentivise better solutions, but that would work best if it was an ongoing discussion in which others also had the opportunity to express their preferences and constraints.

For comparison, I participated in a discussion organised by the Swiss Federal Chancellery,[1] in which they invited dozens of technical experts to participate in weeks of discussion about the future of e-voting in Switzerland. I am not suggesting that the ACT needs something that extensive (unless you decide to continue with Internet voting), but something similar on a smaller scale would help.

I suggest that the most urgent priority for ACT election integrity is a paper-based evidence trail for the pollsite e-voting system—I have detailed some specific suggestions in Section 2. I am omitting Internet voting for now, reiterating my recommendation that it stop.

Like T, I would welcome the opportunity to help draft policy or legislation to improve ACT Election conduct.

I begin by repeating the recommendations from our Supplementary Submission.

[1] https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-81198.html

1 Recommendations from our (supplementary) submission

We recommend that ACT Electoral law be amended to ensure:

1. that in order to have some chance of detecting the most serious errors and vulnerabilities, electronic voting code and system documentation be made openly available for public inspection, at least six months before the election, including:
    (a) e-voting code,
    (b) paper ballot scanning code,
    (c) counting code,
    (d) electoral roll mark-off code, (due to its involvement in privacy issues in the 2008, 2012, and 2016 elections),
    (e) system requirements documentation,
    (f) system design documentation,
    (g) system test plans and test results,
    (h) system accuracy, integrity, and privacy audits, and
    (i) any relevant changes to the interpretation of electoral legislation;
2. that all system modifications, audits, and declarations be completed before candidate nomination closes, with any changed code, documentation, and legislative interpretations publicly released;
3. that the pollsite e-voting system have a voter-verifiable paper record, so that an immutable record of the vote can be verified by the voter independently of the software;
4. that when the electronic preferences are published, there should be a thorough, public, statistical audit of the *paper ballots*, whether filled in by hand or printed by EVACS; and
5. that Internet voting be discontinued, due to the high levels of risk involved in current Internet voting technology.

"Openly available" means without a confidentiality deed.

2 Further details: voter-verifiable paper records and a public audit of them

This section expands on Points 3 and 4 above. They fit together to produce an evidence trail linking the voters' intentions with the published preferences. At this point I ignore the question of whether the votes are properly *counted*: now that we have an open-source independent implementation,[2] it is less important whether the official *counting* code has further errors, because these can be immediately identified by independent parties. I concentrate here on whether the electronic votes accurately reflect the voters' intentions.

Main goal: The main goal is to build an evidence trail from the voters' intentions to the public digitized preferences. This evidence trail should allow verification by voters and scrutineers.

Recommended legislative change: The evidence trail should be specified in two steps:

1. a voter-verified *paper ballot*, so the voter can check that their vote was recorded as they intended;
2. a rigorous, public, audit of randomly selected paper ballots, to compare each ballot against its electronic record and check for discrepancies.

In the current system, citizens who vote on paper can check that their vote reflects their intentions (Step 1), but nobody can check that it is accurately digitized. If the person votes by computer, neither of these verification steps is possible.

2.1 Background

The abolition of paperless e-voting machines in polling places has been a matter of extensive public discussion and scientific examination in the USA, where they are called "paperless DREs," and are rightly recognised as a point of serious vulnerability to errors and fraud. See for example this letter from NYU's Brennan Centre for Justice.[3] The ACT's paperless Direct Recording Electronic machines are not fundamentally different from the ones that most US states have recently abolished.

In the USA, both the design of the paper record and the precise methods for auditing have been the subject of extensive research. For example, some research indicates that for US-style ballots, voters do not adequately check paper printouts[4]—this research suggests that in the US, voters should manually complete a paper ballot, with a pollsite scanner to alert them to accidental informal votes. It is not clear how well this research translates to Australia, because our ballots are very different. I recommend some empirical testing of whatever solution is adopted, to see how well voters detect errors.

There is a vast literature on rigorous statistical audit methods for elections. These are distinct from software audits: they compare voter-verified paper ballots with their electronic representations. The best of these methods are called

[2] `https://github.com/SiliconEconometrics/PublicService`

[3] `https://www.brennancenter.org/our-work/research-reports/letters-urging-states-secure-replace-paperless-dre-voting-machines`

[4] `https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf`

"Risk Limiting Audits," and were pioneered by Philip Stark at UC Berkeley. Some US states, such as California, now require Risk Limiting Audits as part of their electoral law.[5]

My research group has been at the forefront of extending these methods to complex electoral systems including the preferential systems used in Australia[6] (joint work with Michelle Blom, Philip Stark, Peter Stuckey and Damjan Vukcevic). See for example our paper about our world-first preferential risk-limiting audit pilot in San Francisco[7]. At present there is no known Risk Limiting Audit method for the single transferable vote systems used in the ACT and most of Australia's upper houses. However, a public audit would still provide an indication of the rate of error, which would help to inform further steps. No other Australian jurisdiction has adequate audit legislation in place, but they all need it.

2.2 Specific possibilities

There are several different forms this evidence trail could take in the ACT, each with different tradeoffs for convenience, privacy, cost, etc. Some examples:

- Citizens could vote on paper with a pencil (like we do in the Senate), then the ballots could be centrally scanned.
- Citizens could vote on paper with a pencil, then scan their ballot in the polling place.
- EVACS could be modified to print out a paper ballot rather than retaining the vote electronically. Voters would check their printout and deposit it in a cardboard ballot box with the manually-completed ballots. Then a central scanner could digitise them all.
- EVACS could be modified to print out a paper ballot and also retain the vote electronically. Voters would put their paper ballot in a special ballot box (distinct from the manually-completed ones).

The auditing step would be performed publicly in the presence of scrutineers, and also requires careful design in order to be valid. Roughly, it would consist of taking random samples of the paper ballots and comparing their contents with the corresponding electronic preferences. Any discrepancies would need to be noted, with some escalation if the rate of error seem unacceptably high.

All these design decisions have complex tradeoffs involving integrity, privacy, cost, convenience, etc. But in all cases, the theme is to return the responsibility for election scrutiny to candidate-appointed scrutineers, ensuring they see enough evidence to be convinced that the election outcome is right.

I would be very happy to work with the committee on drafting some improved legislation, on this theme or any others.

[5] https://www.sos.ca.gov/administration/regulations/current-regulations/elections/risk-limiting-audits

[6] https://arxiv.org/abs/1903.08804

[7] https://arxiv.org/abs/2004.00235