LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

STANDING COMMITTEE ON JUSTICE AND COMMUNITY SAFETY
Mr Peter Cain MLA (Chair), Dr Marisa Paterson (Deputy Chair), Mr Andrew Braddock MLA

Submission Cover Sheet

Inquiry into Electoral and Road Safety Legislation Amendment Bill 2023

Submission Number: 007

Date Authorised for Publication: 02 August 2023

Submission to the Inquiry into Electoral and Road Safety Legislation Amendment Bill 2023

Dr. Andrew Conway
Independent Researcher
he/him pronouns

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

[redacted]

Mx. T Wilson-Brown
Independent Security Researcher
they/them pronouns

[redacted]

July 28, 2023

The ACT electoral process is unique in current Australian practice in that the overwhelming majority of votes come through a process that cannot be effectively scrutinised. Electronic voting without a paper trail and, even worse, internet voting, create a way for external attackers or dishonest insiders to change a very large number of votes with low—or zero—risk of detection. Even if the election result is accurate, it may be difficult or impossible to provide sufficient evidence that the votes were handled correctly. The execution of every stage of every voting and counting system needs to be verifiable for the result to be trustworthy. In the absence of evidence that the results are right, any disgruntled candidate or conspiracy theorist could challenge the result, and Elections ACT may not be able to repudiate their claims.

For protection of ACT's democracy against foreign interference, corruption, and bored teenage hackers, use of voting systems without a human readable paper trail should be banned.

The basic problem is the same whether the unverifiable system is connected to the Internet or not: interference can be undetectable in practice. This means that voters cannot tell whether their vote is accurately recorded, while scrutineers cannot tell whether votes are properly recorded and included. What makes ACT elections particularly vulnerable is the huge numbers of unverifiable votes. No other Australian jurisdictions, and very few other democracies in the world (excluding Brazil), take the overwhelming majority of votes through a system

that voters and observers cannot check. Running elections over the Internet increases the ease of attack, but doesn't fundamentally alter the threat—if anything, the pollsite system is more dangerous because it takes the huge majority of votes.

The assurances from Elections ACT—that the outcome is trustworthy because the Australian Signals Directorate or the Australian Cybersecurity Centre have endorsed the code—miss the point (even if they are true). The system is inherently brittle because, in the event of a compromise, misrecording of votes could be undetectable. Malware on remote personal devices that individuals use to vote online could misrecord their votes before they are sent to the server.[1] Similarly, even if the EVACS software itself is perfectly secure and absolutely correct, physical or electronic security problems at the polling place (or before the computers arrive at the polling place) could allow it to be substituted. In the last election, there were errors in Elections ACT's vote counting code—it is not credible that they can guarantee the security and correctness of all code and devices used in either pollsite or Internet voting.

Voter impersonation is one vulnerability that is much easier to exploit over the Internet. Although it is possible to falsely represent another voter at a polling place, the opportunity to do so in an automated way, at scale, from outside Australia, using leaked credentials from data breaches such as the Optus breach, makes the attack potentially much more severe against an Internet voting system than a pollsite one.

We do not understand the ACT government's response to JACS's previous recommendations for improving the transparency, verifiability and integrity of the electoral process. The government's response stated that these requirements were "a matter for the Electoral Commission." This included Recommendation 5 (a voter-verifiable paper record for the pollsite electronic voting system), Recommendation 6 (a public audit of electronic vote records against their corresponding paper record to check for discrepancies), and Recommendations 9 and 10 (availability of source code and system documentation). Recommendations 7 ("that the ACT Government assess the benefits and risks of providing an online voting system...") and 11 ("that the Electoral Act require public release of the electronic voting code and system documentation...") were supported in principle but, as far as we can tell, never actioned. Instead, the bill contains an expansion of Internet voting and not one single measure for improving—or even assessing—security, transparency, accuracy, privacy or integrity of any part of the electoral process.

Road safety could also be called "a matter for City Services", but it is the Assembly's responsibility to legislate for basic safety standards. Similarly, most jurisdictions legislate basic standards of transparency, privacy, security and integrity for voting systems. Some of these standards exist in the current Electoral Act, but they are not effectively monitored or enforced. External experts have discovered multiple security and counting issues, despite internal

[1] The NSW iVote system was demonstrated to be vulnerable in 2015 to the injection of malware that could implement this attack `https://arxiv.org/abs/1504.05646`.

reviews and testing, and external audits.

Very few other jurisdictions continue to allow paperless direct recording electronic voting machines—no other Australian state allows them for general voting, though some permit them for voters with disabilities, making them a small fraction of the overall vote count. Most US states have now disallowed them for general voters, requiring some form of paper ballot instead.

The only comparable Australian experiment on election security is the NSW iVote system which, despite consistent warnings from us and numerous other security experts, continued to be used for internet voting from 2011 to 2021. The system suffered substantial downtime through the last two days of polling in local government elections in 2021, leading to a Supreme Court decision to void 3 local council outcomes. This decision was based on optimistic estimates from the NSW Electoral Commission—based on our quantative analysis, more than 30 other outcomes could also be in doubt. NSW discontinued iVote and successfully ran their 2023 state election without it.

There is no known way of adequately securing voting over the Internet while preserving voter privacy. There are, however, practical ways of verifying and auditing pollsite voting. These include the measures we recommended previously, which were reiterated by JACS as their Recommendations 5 and 6: provide a voter-verifiable paper evidence trail, then audit it to ensure that the electronic votes accurately reflect it.

Internet voting aims to enfranchise remote voters similarly to pollsite voters. The security and privacy requirements in the current Electoral Act are the same, regardless of the voting system.

Internet voting can enfranchise some remote voters, some of the time, but it can't be reliably secured. So their franchise can be removed by external bad actors, or in extraordinary circumstances, the Electoral Commission or their corporate partners. Internet voting downtimes are common—they can be caused by unexpected vote volumes, system misconfigurations, or external interference. Downtimes remove the franchise from voters, with no warning, and no fallback voting method. But downtimes can also be triggered by malicious actors, to hide other kinds of interference with the voting system.

It is the responsibility of elected legislators in each democracy to set the rules for trustworthy elections. The current bill does not adequately discharge that responsibility.

1 Recommendations for ensuring ACT Election security (from Submission 1)

This list of recommendations the same as our previous submissions.

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 immediately after the electronic preferences are published, there should be a thorough, public, statistical audit of the *paper ballots*[2], 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]Like COMMONWEALTH ELECTORAL ACT 1918 - SECT 273AC, *Ballot paper sampling assurance throughout computerised scrutiny of votes in Senate election*, although we would add a requirement that the ballots tested be chosen randomly to avoid warning hackers which votes not to change.