



**LEGISLATIVE ASSEMBLY**  
**FOR THE AUSTRALIAN CAPITAL TERRITORY**

---

**STANDING COMMITTEE ON JUSTICE AND COMMUNITY SAFETY**

**Mr Jeremy Hanson MLA (Chair), Dr Marisa Paterson (Deputy Chair), Ms Jo Clay MLA**

## Submission Cover Sheet

Inquiry into 2020 ACT Election and the Electoral Act

**Submission Number: 020**

**Date Authorised for Publication: 5 May 2021**

Supplementary Submission to the Standing  
Committee on Justice and Community Safety's  
Inquiry into the 2020 ACT Election and the  
Electoral Act

Dr. Andrew Conway  
Independent Researcher  
he/him pronouns

Dr. Thomas Haines  
NTNU  
he/him pronouns

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

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

April 30, 2021

This submission considers further information on the implementation, security and transparency of electronic voting that has emerged since our first submission.

We would be happy to discuss any of these matters with the committee.

# 1 Count Errors

We were very surprised to hear the Electoral Commission tell the ACT’s Standing Committee on Justice and Community Safety

*A lot of the issues that have been raised go to six decimal places. Prior to the election in July the Electoral Act was changed to implement rather than rounding to the nearest whole number to rounding to six decimal places when we are talking about vote values. So the discrepancies are in the realms of those six decimal places.*<sup>1</sup>

We had clearly communicated to Elections ACT that some errors were on the order of 20 votes, with the potential for much larger discrepancies due to the algorithmic nature of the coding error.

It is hard to attribute this omission to an accidental mistake, because it was repeated in response to a followup question:

*MS CLAY: When you say you are rounding to within six decimal places, do you mean that the anomalies are probably less than an entire vote? They are in the order of 1/1000th or 1/10,000th, is that what you are saying?*

*Mr Spence: Without being able to generalise for every occurrence, that is very much where we are talking about.*<sup>2</sup>

Although some anomalies were as small as the sixth decimal place, some were much larger. We do not understand why Elections ACT did not mention those larger errors in their answers.

Nevertheless, we are glad to see that Elections ACT have now made the necessary corrections. An example from Murrumbidgee is shown below—Figure 1 shows the tallies for Greens candidate Emma Davidson, as they were given on Elections ACT’s website<sup>3</sup> soon after the election (2020). Figure 2 shows corrections made to the official tallies in March 2021, consistent with our recommendations. In this example, Emma Davidson has gained 16 votes.

The commission’s report on the 2020 election describes the detailed testing they performed for the change to rounding to 6 decimal places. Similar testing would have detected the larger algorithmic error, particularly if it included a comparison to past casual vacancies, or past elections. Based on multiple recent FOI requests, it appears that the commission does not prepare detailed

---

<sup>1</sup>ACT Legislative Assembly, Standing Committee on Justice and Community Safety, inquiry into annual and financial reports 2019–2020 and ACT budget 2020–2021, 19th February 2021 <http://www.hansard.act.gov.au/hansard/2021/comms/jacs01a.pdf>

<sup>2</sup>*ibid.*

<sup>3</sup>From Elections ACT’s website: [https://www.elections.act.gov.au/elections\\_and\\_voting/2020\\_legislative\\_assembly\\_election/distribution-of-preferences-2020](https://www.elections.act.gov.au/elections_and_voting/2020_legislative_assembly_election/distribution-of-preferences-2020), Murrumbidgee table 2.

1	ACT Legislative Assembly Election 2020 - F		
2	The ACT Greens		
3	Count	Terry BAKER	Emma DAVIDSON
55			120.000000
56	27		7543.575540
57			588.000000
58	28		8131.575540
59			11.000000
60	29		8142.575540
61			30.676259
62	30		8173.251799
63			1113.710876
64	31		9286.962675
65			-328.962675
66	32		8960.000000

Figure 1: Emma Davidson’s official tallies at the time of the election (2020).

1	ACT Legislative Assembly Election 2020 - F		
2	The ACT Greens		
3	Count	Terry BAKER	Emma DAVIDSON
55			120.000000
56	27		7543.575538
57			591.000000
58	28		8134.575538
59			30.676258
60	29		8165.251796
61			1138.000000
62	30		9303.251798
63			
64			
65			
66			

Figure 2: Emma Davidson’s corrected official tallies, with 16 more votes, from March 2021.

acceptance test plans for its voting and counting systems.<sup>4 5 6</sup> So voting system changes may be accepted after bespoke tests, or in the absence of any tests. But best practice involves running a reliable, repeatable test suite, after every change to the system.

We will not dwell upon the counting errors, except to say that they show that existing processes do not guarantee the accuracy or security of the software on which ACT election outcomes depend. The rest of this submission instead focuses on what this experience implies for the legislative change necessary to ensure future ACT Elections are conducted in a trustworthy fashion.

Our recommendations remain similar to our first submission. They are listed in full at the end of this submission. Since our first submission, more information has been made available under FoI that adds support to these recommendations.

## 2 Audits

The current auditing processes do not adequately examine the software systems. We know of several errors that went undetected in the counting module. There could be multiple errors in the pollsite evoting, Internet voting, or paper ballot scanning modules that went undetected throughout the electoral process.

<sup>4</sup>[https://www.righttoknow.org.au/request/vote\\_secrecy\\_in\\_2020\\_election#incoming-19178](https://www.righttoknow.org.au/request/vote_secrecy_in_2020_election#incoming-19178)

<sup>5</sup>[https://www.righttoknow.org.au/request/audit\\_documents\\_for\\_the\\_2020\\_eva#incoming-19177](https://www.righttoknow.org.au/request/audit_documents_for_the_2020_eva#incoming-19177)

<sup>6</sup>[https://www.righttoknow.org.au/request/paper\\_vote\\_scanning\\_accuracy\\_in#incoming-20365](https://www.righttoknow.org.au/request/paper_vote_scanning_accuracy_in#incoming-20365)

The Electoral Commissioner told the ACT’s Standing Committee on Justice and Community Safety that

*... the code underlying the electronic voting and counting system goes through a series of tests and certifying procedures, both internal to the commission [and] through our vendors who work with us to develop the system and provide it to us and in turn to the independent certifying process to ensure that the code functions as it is intended in accordance with the law to deliver the result as intended by the votes cast.*

However, this characterisation is not supported by documents released under FoI, in which the auditors (BMM Australia) state that “BMM did not perform tests on the current software version,” and “It was not the purpose of the review to verify that the code works correctly.”<sup>7</sup>

\$60,000 is a lot of money for an audit that doesn’t even certify the legally required correctness, security, and secrecy properties of the system.

This supports our recommendation that the code and related documents be made openly available to public scrutiny, rather than entrusted to small number of auditors chosen by Elections ACT.

### 3 Privacy

Elections ACT’s 2020 election report makes no mention of vote privacy, despite the significant effort they put into improving vote privacy during the development of the 2020 election systems.<sup>8 9</sup>

As we mentioned in our previous submission, the voting system audits do not cover vote privacy. The auditors only certify “that the code matched the documented scope of the eVACS system and that no malicious code had been introduced that could insert, alter or delete ballot information unlawfully.”

In addition, privacy is a property of a system in context. From 2008-2016, some electronic votes in ACT elections could be revealed using data from multiple election systems. Specifically, the systems that collected roll mark-off times and electronic voting times.<sup>10 11</sup> Isolated audits of individual systems are unable to detect these kinds of errors.

Unfortunately, we were unable to fully analyse vote privacy in the 2020 election, because we did not have enough information about all the relevant systems.

---

<sup>7</sup>[https://www.righttoknow.org.au/request/request\\_for\\_the\\_audit\\_documentat](https://www.righttoknow.org.au/request/request_for_the_audit_documentat)

<sup>8</sup>Page 16 of <https://www.righttoknow.org.au/request/6776/response/19178/attach/7/HAZOPSV1.0.pdf>

<sup>9</sup>Page 9 of <https://www.righttoknow.org.au/request/6776/response/19178/attach/8/SecurityandEVACSv1.1.pdf>

<sup>10</sup>Page 16 of <https://www.righttoknow.org.au/request/6776/response/19178/attach/7/HAZOPSV1.0.pdf>

<sup>11</sup><https://github.com/teor2345/Elections2018/blob/master/ElectionsACTDisclosure.md#vulnerability-summary>

We were unable to access any information about the roll mark-off system via FOI. However, the publicly released voter frequency data shows that at least one system was collecting voter times across all polling booths. This increases the risk of vote disclosure, particularly if there are mistakes in the design or implementation of any of the vote-handling systems.

We were able to access eVACS security review, system requirements, and design documents via FOI. It appears that the proposed changes are intended to preserve polling booth electronic vote privacy. However, we were unable to verify that these changes were implemented correctly, because we did not have access to the eVACS system source code.

We were able to access some information about the Internet voting (OSEV) system via FOI. But there was not enough information to analyse vote privacy for overseas voters, because we did not have access to the OSEV system source code.

Given the errors we discovered in the counting system in 2020, and in vote privacy from 2008-2016, it is possible that some vote privacy issues remain, particularly in the OSEV system.

This supports our recommendation that the code and related documents be made openly available to public scrutiny, rather than entrusted to small number of auditors chosen by Elections ACT.

## 4 Paper Vote Scanning

The Electoral Commission’s report on the 2020 election makes the claim that

*While it is possible that errors have occurred on individual ballot papers across these recent electoral events, the fact that across a combined 9000 ballot papers not a single error has been identified indicates that the ballot paper scanning system provides for a very high level of counting accuracy.*

However, the current paper vote scanning audit processes are not sufficient to guarantee the accuracy of the system.

Specifically, the checks and audits performed by the commission are unable to detect certain kinds of errors.

There are no checks for ballot papers that are actually informal, but scanned as formal. In response to a recent FoI, the commission stated that “a ballot paper that contains ‘errors’ in its formality or consecutive numbering, or a ballot paper that contains ambiguous numbering, is identified during verification stage 1 and moves to verification stage 2 for manual checking.”<sup>12</sup> Because ballots that scan without errors are accepted without further checks, some informal ballot papers might be accepted by the system, due to a mis-scan that happens to make them appear formal.

---

<sup>12</sup><https://www.righttoknow.org.au/request/7099/response/20365/attach/4/ReasonsfordecisionEACTF01220221.pdf>

Paper ballot checks are rare. Typically, checks are performed on scanned images, rather than the original paper ballots. And post-election audits only use scanned images.<sup>13 14 15</sup> Therefore, these checks are unable to detect certain kinds of scanner errors. For example: a scanner swaps two valid numbers, or substitutes an incorrect number that happens to be valid. In 2013, these kinds of scanner substitutions were discovered by researchers in Xerox scans of architectural plans.<sup>16</sup>

Before any manual checks are performed, the scanning error rate is at least 1.2%. In 2020, 944 ballots were corrected in phase 2, from a total of 77,884 paper ballots.<sup>17</sup> (The correction statistics for other phases are not available, so the actual error rate could be much higher.) Given this base error rate, it is very unlikely that the other phases could discover all the remaining errors.

The commission’s characterisation is also not supported by documents released under FoI, in which the auditors (BMM Australia) state that “the hardware changes are not implemented in the source code”, “BMM reviewed the design documentation and performed a code review” and “It was not the purpose of the review to verify that the code works correctly.”<sup>18</sup>

This supports our recommendation that the code and related documents be made openly available to public scrutiny, rather than entrusted to small number of auditors chosen by Elections ACT. Based on this new information about the scanning system, we also recommend thorough, publicly verifiable, audits of the *original paper ballots* in the presence of scrutineers.

## 5 Access to source code

Thomas Haines requested access to the overseas e-voting (OEV) source code on the 6th of October 2020; on the 25th of February 2021 (142 days later) the Electoral Commissioner sent a letter saying the commission had decided to allow access. However, as of the 28th of April 2021 the source code is not accessible.

The confidentiality deed contains numerous problematic provisions, including considerable ambiguity over when and whether the researcher may report problems to the public.<sup>19</sup> Vanessa Teague requested access to the EVACS voting module code on 17th September 2020, when Elections ACT’s website still con-

<sup>13</sup><https://www.righttoknow.org.au/request/7099/response/20365/attach/9/3.ACTECBallotScanningReport.pdf>

<sup>14</sup><https://www.righttoknow.org.au/request/7099/response/20365/attach/10/4.AuditofScanning2020election.pdf>

<sup>15</sup>[https://www.righttoknow.org.au/request/paper\\_vote\\_scanning\\_accuracy\\_in#incoming-20365](https://www.righttoknow.org.au/request/paper_vote_scanning_accuracy_in#incoming-20365)

<sup>16</sup><https://www.pcworld.com/article/2046047/xerox-scanners-found-to-sometimes-alter-numbers.html>

<sup>17</sup><https://www.righttoknow.org.au/request/7099/response/20365/attach/9/3.ACTECBallotScanningReport.pdf>

<sup>18</sup><https://www.righttoknow.org.au/request/7099/response/20365/attach/12/6.BallotPaperScanningSystemCertificateBMM.pdf>

<sup>19</sup><https://www.righttoknow.org.au/request/6754/response/18704/attach/4/EACTConfidentialityDeedPollProvisonofEVACScode.pdf>

tained strong language about transparency and open scrutiny. Elections ACT refused requests to alter some unacceptable terms of the confidentiality deed.<sup>20</sup> So in practice the code is not available, for two main reasons:

- the terms of the confidentiality deed would be unacceptable to many researchers, for example due to the ethical problem of possibly preventing public disclosure during the election period;
- Elections ACT may refuse to allow access, even to researchers who agree to sign the confidentiality deed.

This supports our recommendation that the code be made openly available to public scrutiny, in a timely manner, on a timescale which would allow any errors to be corrected before the election result becomes final. “Openly available” means without a confidentiality deed.

## 6 Engagement with researchers

The ACT Electoral commissioner told the ACT’s Standing Committee on Justice and Community Safety

*I have undertaken to work with Associate Professor Teague to continue to examine the nature of her assertions. ... we will continue to work with Dr Teague and her colleagues.*

This is not accurate—we did initially offer to meet with Elections ACT, including with Mr Cantwell, but no such offer was accepted. Mr Cantwell later made an indication by email that Mr Spence would be willing to meet with us, but our efforts to follow up and find a time did not get a response. We have received no further communication since Mr Cantwell made this statement to the committee.

We do not think it would be beneficial to force Elections ACT to meet with us if they do not wish to. However, we believe it is important to reconsider the incentives and legal requirements for ACT election conduct, to ensure that officials are motivated to engage with people who understand election security, to improve the conduct of ACT Elections.

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

This list of recommendations is the same as in our first submission, except that we did not know that the scanning system did not include an audit of paper ballots—this has now been added.

---

<sup>20</sup>Specifically, clauses prohibiting the sharing of information about serious problems before the certification of the election results.



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.