LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

SELECT COMMITTEE ON THE 2016 ACT ELECTION AND ELECTORAL ACT
Ms Bec Cody MLA (Chair), Mr James Milligan MLA (Deputy Chair)
Ms Tara Cheyne MLA, Ms Caroline Le Couteur MLA, Mr Andrew Wall MLA,

Submission 22

Name – Lyria Bennett Moses (UNSW), Rajeev Gore (ANU) and Dirk Pattinson (ANU)

Submission to the ACT Select Committee On 2016 ACT Election and Electoral Act

Lyria Bennett Moses, UNSW Sydney, [redacted]

Rajeev Goré and Dirk Pattinson, Australian National University

[redacted]

June 30, 2017

1 Preamble

We commend ACT Elections for their reasoned way of dealing with election issues in the ACT. We thank the ACT Parliament for the opportunity to contribute to the inquiry as domain experts.

The ACT is ahead of other jurisdictions in Australia in using computers to assist in electoral matters (in particular, vote counting). For example, ACT Elections provides open access to the computer code used in counting elections which enabled us to expose some errors in the code so that they could be repaired by the software vendor. This contrasts with the Electoral Commission of New South Wales or the Australian Electoral Commission, where the computer code is deliberately kept secret, and where post-hoc analyses have uncovered significant errors [4].

We also commend ACT Elections for its cautious view of internet voting, a technology that, despite best efforts, is known to be fraught with severe security problems [15, 8].

In this submission, we contribute our expert technical and legal opinion to matters surrounding use of computers in elections in the ACT, and hope that our contribution will further the discussion and lead to even more transparent, fair and accountable elections in the ACT. We would be happy to appear in person at the inquiry: please contact Professor Goré via email.

2 Recommendations

Recommendation 1: That ACT Elections should begin a consultation process to remove the various “simplifications” in the current Hare-Clarke system, which can lead to strange results [7] and which are no longer necessary since all counting is done by computer and the “simplifications” were added only to make hand-counting easier.

Recommendation 2: That ACT Elections replace rounding, not by fractions to 6 decimal places as recommended by ACT Elections, but by exact counting of fractional votes, which we have shown to be both possible and practical.

Recommendation 3: That ACT Elections resists rolling out an internet voting system because all such systems to date are inherently insecure.

Recommendation 4: That ACT Elections should consider the repercussions of a formal challenge from a losing candidate to the results of an election: specifically, how would ACT Elections prove that the electronic count was correct and that it was properly able to be scrutinised by eligible organisations as required by the ACT Electoral Act.

Recommendation 5: That ACT Elections should replace the current eVACS vote-counting module with a module that guarantees independent verifiability of the final result, both to build public trust and so that the counting software cannot be faulted in a court challenge.

Recommendation 6: That ACT Elections should conduct a post-election audit of the paper ballots against the published preference data files to ensure that the counted electronic ballots do indeed represent the paper ballots.

3 Background

Use of Computers in ACT elections. In 2001, ACT Elections were one of the first to use electronic vote-casting and vote-counting for binding elections and are to be congratulated for their foresight. Given their limited budget, ACT Elections and the company involved have done a remarkable job of procuring the eVACS system. To put that into perspective, consider that the electoral commissions in the United States wasted millions of dollars buying electronic voting machines which were subsequently found to contain massive security holes [9]. The original eVACS system has been modified to replace manual entry of ballots with automatic optical character recognition for data entry, but the basics of how vote-casting and vote-counting operate have remained essentially the same.

Independent Verifiability of Election Results. Since 2001, academic researchers in electronic voting have developed the notion of end-to-end voter-verifiable (E2EVV) systems [3]. The basic idea is that modern electronic voting systems should provide *at least* the same degree of scrutiny enjoyed by vote-casting of paper ballots and hand-counting of paper ballots. Indeed there is even a non-profit foundation [5] whose aims are to "safeguard elections in the digital age".

For example, voters know that the paper ballot that they put into a ballot box is exactly what they intended since they create the ballot directly with a pencil. Scrutineers from various interest groups can watch election officials conduct a hand-count of paper ballots, and theoretically, the validity of each paper ballot can be checked in this way (if time and resources permit). Finally, there are checks and balances in place to ensure that ballot boxes are not tampered with or lost, which is how the debacle in Western Australia was discovered.

The Holy Grail of e-voting research is that electronic vote-casting and electronic vote-counting should give at least the same guarantees, and in fact improve scrutiny, as some physical limitations, such as the number of observers being able to fit into a room, are no longer applicable.

Current use of eVACS. We are concerned that the software used by ACT Elections meets none of the requirements of modern E2EVV voting. Specifically:

Vote-casting: there is no guarantee that the ballot recorded by eVACS is actually the same as the ballot that was displayed to the voter and there is no guarantee that the ballot created by the OCR scanner is actually identical to the paper ballot that was scanned;

Vote-counting: there is no guarantee that the vote-counting module of eVACS actually counts ballots correctly according to the ACT Hare-Clake scheme. We have analysed the vote-counting module of eVACS and, since 2001, we have identified at least three bugs in this module [10]. Each bug was acknowledged by ACT Elections (see `http://www.elections.act.gov.au/elections_and_voting/electronic_voting_and_counting`), and each was fixed by the vendor. We demonstrated that, for each bug, we could design an election in which the bug led to an error in the counting result. We stopped scrutiny after finding the third bug: so how can we be sure that there are no further bugs?

Legal Challenge: there are no precedents for how the High Court would treat electronic vote-casting and vote-counting. Consequently, it is perfectly possible that a high-court challenge to the results of an election result could lead to an ACT election becoming a fiasco.

The Need for Verifiability. Even if technical guarantees for the functional correctness of eVACS can be given, and the source code and formal guarantees for its correctness were available, its operation in a particular election is effectively a "black box", and the lack of verifiability precludes building a large base of public trust. How can we be sure that the code used to count the votes was actually the code of eVACS and not some code inserted by a malicious insider?

While subjective trust cannot be guaranteed through greater transparency [11], transparency about both electronic vote-casting and electronic vote-counting in a particular election are important in reducing errors and ensuring an accurate count, promoting public trust and providing the evidential basis for demonstrated trustworthiness. In particular, it is a lack of transparency that has been the primary source of criticism of existing systems, both in the literature [2, 4] and among civil society organisations [14] such as `blackboxvoting.org` and `trustvote.org`. International commitment to transparency is also demonstrated through initiatives such as the Open Government Partnership.

Another important concept referred to both in the literature and by civil society organisations is public accountability which requires giving an "account" or explanation to the public as well as being held publicly responsible for failures, in particular when called on (for example, in court). In our most recent work [6], we have shown how to generate the computer code for counting electronic ballots exactly, with no approximations or rounding involved, and such that the count is fully verifiable: any interested party can hire an undergraduate programmer to write a computer program to check the certificate produced by our vote-counting program against the published ballots to ensure that the result is correct. We have also shown that writing such a checker is simple and inexpensive, so each interested party could do it independently.

Hand-counting provisions in the ACT Hare-Clarke Act. To make hand-counting easier, the ACT Hare-Clarke Act adds a number of "features" to what might be called a standard version of single-transferable voting: "the last parcel" and "rounding fractions to their nearest integer values" to name just two. We have shown that these features lead to strange results: for example, the nonsensical situation where candidates have negative numbers of votes during the count, and even the election of the wrong candidates [7]. Moreover, we have given a simpler form of Hare-Clarke and built matching counting code for this version, and shown that it does not suffer from such strange behaviour [7].

Security of Internet Voting. The concerns voiced above are not related to the possibility of the eVACS systems being "hacked" in any way. Thus the fact that eVACS is not connected to the internet does **not** assuage our concerns.

While the roll-out of internet voting would possibly increase voter participation, the risks associated with internet voting are significant and are by no means justifiable. For example, the iVote system used in the state of New South Wales has been found to be vulnerable to an extent where the number of possibly compromised ballots were larger than the margin of winning for one candidate [8]. Similarly, a (mock) trial of a security analysis carried out for an internet voting system in Washington D.C. [15] allowed intruders to get full access to the system within two days, and has led to the system not being used for legally binding elections.

Most importantly, the discovery of attempts to influence the recent US Presidential Election means that the High Court is unlikely to accept the standard governmental response that "there is no evidence of any tampering" since good hackers will cover up their tracks. Indeed, the break-in to the proposed electronic voting system in Washington, D.C. [15] was *only* discovered because the academic intruders purposefully changed the system so that it would play the University of Michigan "fight song" after each ballot was cast!

Post-election Audits Engender Scrutiny. Another avenue to engender trust is to conduct a post-election audit of the paper ballots whereby a randomly chosen sample of paper ballots are compared against their digital counterparts [12]. The amount of work increases with the degree of confidence required but is usually significantly less than a full hand-count. It has been demonstrated how to conduct such audits for single-transferable voting [1]. The main requirement is an efficient way to locate a given randomly chosen ballot from the pile of paper ballots. This has been successfully carried out for Danish council elections [13].

4 About the Authors

Lyria Bennett Moses is an Associate Professor in the Faculty of Law at UNSW Sydney. Lyria's research explores issues around the relationship between technology and law, including the types of legal issues that arise as technology changes, how these issues are addressed in Australia and other jurisdictions. Lyria is currently a Key Researcher and Project Leader on the Data to Decisions CRC, exploring legal and policy issues surrounding the use of data and data analytics for law enforcement and national security. Lyria is also Chair of the Australia Chapter of the IEEE Society for the Social Implications of Technology, Chair of the Law, Technology and Innovation Research Network at UNSW Law and a PLuS Alliance Fellow.

Rajeev Goré is a professor of computer science at the ANU Research School of Computer Science. He is an expert in the use of formal methods for software engineering, particularly to verify that a computer program meets its intended specification. With colleagues, he has analysed the computer counting module of the eVACS electronic vote-casting and vote-counting system used by Elections ACT, and also analysed the ACT Hare Clarke Act. He is on the programme committee of The International Conference for Electronic Voting `https://www.e-vote-id.org/`

Dirk Pattinson is an Associate Professor in the Research School of Computer Science at the Australian National University. His research is centred around formal logic, software reliability and certifiable programs, i.e. programs that provide not only an output, but also a certificate that attests to the correctness of the computed results. With collaborators, he has demonstrated that vote counting, including various systems of single transferable vote, can be implemented to produce correctness certificates for real-world elections.

Professor Rajeev Goré
[redacted]

References

[1] M. L. Blom, P. J. Stuckey, and V. J. Teague. Towards computing victory margins in STV elections. *CoRR*, abs/1703.03511, 2017.

[2] M. A. Carrier. Vote counting, technology, and unintended consequences. *St Johns Law Review*, 79:645–685, 2012.

[3] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, 2004.

[4] A. Conway, M. Blom, L. Naish, and V. Teague. An analysis of New South Wales electronic vote counting. In *Proc. ACSW 2017*, pages 24:1–24:5, 2017.

[5] V. V. Foundation. Verified voting foundation, 2003.

[6] M. Ghale, R. Goré, and D. Pattinson. A formally verified single transferable vote scheme with fractional values, Submitted.

[7] R. Goré and E. Lebedeva. Simulating STV hand-counting by computers considered harmful: A.C.T. In *Electronic Voting - First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings*, pages 144–163, 2016.

[8] J. A. Halderman and V. Teague. The New South Wales iVote system: Security failures and verification flaws in a live online election. *CoRR*, abs/1504.05646, 2015.

[9] D. W. Jones and B. Simmons. *Broken Ballots: Will Your Vote Count?* Centre for Study of Language and Information, Stanford University, 2012.

[10] Logic Group at ANU Research School of Computer Science. Formal methods applied to electronic voting systems, 2003. see (`http://users.cecs.anu.edu.au/~rpg/EVoting/`).

[11] O. O'Neill. *A Question of Trust*. Cambridge University Press, 2002.

[12] R. L. Rivest and P. B. Stark. When is an election verifiable? *IEEE Security & Privacy*, 15(3):48–50, 2017.

[13] C. Schürmann. A risk-limiting audit in Denmark: A pilot. In *Electronic Voting - First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings*, pages 192–202, 2016.

[14] F. Vogl. *Waging War on Corruption: Inside the Movement Fighting the Abuse of Power*. Rowman & Littlefield, 2012.

[15] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. Attacking the Washington, D.C. internet voting system. In A. D. Keromytis, editor, *Proc. Financial Cryptography and Data Security 2012*, volume 7397 of *Lecture Notes in Computer Science*, pages 114–128. Springer, 2012.