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: 017

Date Authorised for Publication: 5 May 2021

Electronic Voting Software Is Mission Critical

Rajeev Goré

April 30, 2021

Abstract

Over the past twenty years, my colleagues and I have conducted internationally recognised research on the ACT Electronic Voting system and on the ACT's version of the Hare-Clark Act. Jeremy Dawson and I were part of the original successful bid for the RFC in 2001 and we wrote the prototype for the vote-counting module which demonstrated that a computer could count hundreds of thousands of STV ballots within minutes. Our module was designed to be formally verifiable using modern computer-aided verification tools, but such verification was deemed inessential and our module was replaced by one written by a commercial software vendor. We have reported many anomalies in the Act and many bugs in the resulting vote-counting module. All bugs have been acknowledged and repaired by Elections ACT but our main recommendation to "do it properly using modern formal verification techniques" has been completely ignored. Moreover, if so many bugs exist in the vote-counting module, how many other bugs exist in the thousands of lines of vote-casting code? Be warned: sooner or later, someone is going to challenge an election result and the current procurement process, the resulting software and ACT Elections will be exposed as a joke.

Recommendations.

1. Forbid any sort of internet election, on any scale.
2. Require that the ACT Hare-Clarke Act be changed to remove the numerous "simplifications" which may have made sense when we counted ballots by hand, but which now demonstrably undermine the accuracy of a computerised count: see [5].
3. Require that electronic voting software is treated as safety-critical since it has the potential to wrongly elect government officials [3].
4. Require that vendors of voting and counting software provide public evidence which can be scrutinised by experts that proves that their software meets the claimed security, privacy and correctness criteria.
5. Require that vendors of voting and counting software make their software publicly available for scrutiny by experts without forcing said experts to sign non-disclosure agreements: after all, if the ACT taxpayer pays for the software then I should be able to scrutinise it!
6. Increase funding to ACT Elections so they can do these things properly!

Introduction. My name is Rajeev Goré and I was an ANU academic in Computer Science from 1994 until the end of 2020, and a professor there from 2011. My specialisation is in formal mathematical logic and I obtained my PhD in 1992 from the University of Cambridge, UK. I have served on the program committees of about 100 international conferences in this area, and most recently, I was a co-chair of the Technical Track of the International Conference on Electronic Voting and Identity (`https://www.e-vote-id.org/`). In March 2021, I was a keynote speaker at the International Conference on Formal Engineering Methods (`https://formal-analysis.com/icfem/2020/`). I am also on the editorial board of the International Journal on Logical Methods in Computer Science (`https://lmcs.episciences.org/page/editorial-board`). All of this is just to say "I know what I am talking about".

Safety-Critical Software The term safety-critical system is typically used to describe software and hardware systems where errors may lead to the loss of life: for example, space missions, nuclear power-stations, commercial aeroplanes and autonomous vehicles (`https://ieeexplore.ieee.org/document/1007998`). Various industries have published rigorous standards through the International Organization for Standardization, a worldwide federation of national standards bodies. These standards must be met by vendors when they provide such safety-critical systems commercially (`https://www.iso.org/obp/ui/#iso:std:iso:14620:-1:ed-2:v1:en`).

Formal Verification Some standards even demand that the software is verified correct against its written specifications using computer-aided verification (CAV) tools to prove properties of the formal specification itself, or to prove that a formal model of a system implementation satisfies its specification (`https://en.wikipedia.org/wiki/Formal_methods`). Multiple such CAV tools are now available but they require significant expertise in using these logic-based tools. Consequently, safety-critical systems are expensive to build!

Automatic Extraction of Formally Verified Code. Using such tools, we have shown how to automatically extract efficient vote-counting code which is formally verified to be correct [4]. We have also shown how to automatically extract other cyber security infrastructure required for secure electronic voting [6].

Electronic Voting and Counting Software Is Safety Critical. The history of governmental elections shows that candidates will attempt to abuse any new technological developments [1]. The electronic governmental elections in Kenya were recently annulled by the courts [2]. As we have seen recently in the US, there are now state actors who are also actively attempting to influence elections. To quote the US Vote Foundation:

> *Elections for public office are a matter of national security. Researchers have shown that every publicly audited, commercial Internet voting system to date is fundamentally insecure. . . . It is currently unclear whether it is possible to construct an E2E-VIV system that fulfils the set of requirements contained in this report. Solving the remaining challenges, however, would have enormous impact on the world.* *US Vote Foundation [3]*

The $64,000 Question. How is it possible for a small Australian company to have solved a problem that is defeating the best academics around the world?

The Only Sensible Answer. The litany of software bugs exposed by us and by Conway *et al.* shows that the current procurement process and the resulting software is deeply flawed. Indeed, the counting code is the only part of the system which we can test against our own independent version by comparing inputs and outputs. The likelihood that serious errors are absent from every other part of the system is absolutely zero!

Be Afraid ... Be Very Afraid! Elections ACT, for too long, has fobbed off the problems in the Act and the bugs in the software as being "minor". The current ACT Elections software is a disaster waiting to happen and leaves the ACT government vulnerable to a formal challenge from a losing candidate. Please let me appear before the committee so I can tell you why!

References

[1] Judith Brett. *From Secret Ballot to Democracy Sausage: how Australia got compulsory voting*. Text Publishing, Melbourne, 2019.

[2] Jason Burke. Kenyan election annulled after result called before votes counted, says court. The Guardian, 20 September 2017, 2019.

[3] US Vote Foundation. The future of voting, 2015.

[4] Milad K. Ghale, Rajeev Goré, Dirk Pattinson, and Mukesh Tiwari. Modular formalisation and verification of STV algorithms. In *Electronic Voting - Third International Joint Conference, E-Vote-ID 2018, Bregenz, Austria, October 2-5, 2018, Proceedings*, pages 51–66, 2018.

[5] Rajeev Goré and Ekaterina 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.

[6] Thomas Haines, Rajeev Goré, and Bhavesh Sharma. Did you mix me? formally verifying verifiable mix nets in electronic voting. *IACR Cryptol. ePrint Arch.*, 2020:1114, 2020.