SUBMISSION TO PARLIAMENT OF VICTORIA ELECTORAL MATTERS COMMITTEE INQUIRY INTO ELECTRONIC VOTING, 2016

Prof Rajeev Goré
Research School of Computer Science
The Australian National University
[redacted]

Dr Vanessa Teague
Computing and Information Systems,
University of Melbourne
[redacted]

This submission addresses security, privacy, transparency and verifiability of electronic voting and vote counting. The submission repeats similar submissions to federal and state inquiries on elections. We would be happy to discuss or expand upon these issues, or any issues raised in our previous submissions.

Prof Rajeev Goré is the leader of the Logic and Computation Group at ANU. His expertise is in using logic to verifying correctness of programs, including those that count votes. He is currently a chief investigator on an Australian Research Council Discovery Grant on verified vote counting.

Dr Vanessa Teague is a senior lecturer at the University of Melbourne. Her expertise is in techniques for verifiable elections, particularly cryptographic techniques. She worked (on a voluntary basis) with the Victorian Electoral Commission on their vVote project. She is currently a chief investigator on an Australian Research Council Discovery Grant on privacy, with an e-voting focus. She is on the advisory board of Verified Voting and is the co-chair of the technical track of E-Vote-ID, Europe's premier technical e-voting conference.

Neither author has any financial interest in electronic voting.

The Computing Research and Education Association of Australasia (CORE), (www.core.edu.au), is an association of university departments of computer science in Australia and New Zealand. We are endorsed by the executive of CORE as experts for the purposes of this submission.

SUMMARY OF RECOMMENDATIONS:

Recommendation 1 [Transparency]: *The system's source code and documentation should be publicly available for open review. This is already true for the VEC's vVote project and vote counting code.*

Recommendation 2 [Verifiability]: *For each election, each voter should get good evidence that his or her vote is cast in the way that he or she intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied.*

Recommendation 3 [Internet Voting]: *Secure and usable remote electronic voting, i.e. Internet voting, remains an unsolved problem. If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.*

Recommendation 4 [Electronic delivery and paper returns]: *We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.*

Recommendation 5 [Cast-as-intended verification]: *secure voting by computer in the polling place is feasible provided it has a human-readable paper trail for sighted voters, or some other form of direct verification, such as the vVote project.*

Recommendation 6 [Counting algorithm verification]: *formal verification that the computer code for (STV) vote-counting correctly implements the count is also possible using modern software verification techniques. This does not remove the need for scrutineers to audit electronic vote data using the paper vote records.*

Our discussion of verifiability and transparency of STV counting and the candidate draw is in a prior submission. We will not repeat it here, but have repeated the main recommendation (Recommendation 6).

INTRODUCTION

The potential advantages of electronic voting are obvious, but the risks are not. Computers could help voters who would otherwise need human assistance, and could protect all voters from accidentally voting informally. However, voters' democratic rights are not enhanced if their votes can be manipulated, the privacy of their vote can be violated, or if the system fails to provide evidence that withstands a legal challenge.

This submission considers two ways of including computers in elections:

1. **Internet voting**
   Secure and usable Internet voting suitable for Australian elections is an unsolved problem.

2. **Electronic voting in a supervised polling place**
   Voters should get direct evidence from a human-readable paper record that their vote is cast as they intended. That evidence should be linked to a meaningful way for scrutineers or observers to check that the votes are included unaltered in the tally. This could be achieved with an end-to-end verifiable system (such as the vVote system) or traditional scrutiny of paper printouts.

The single most important property of any election, whether it is paper-based or computer-based, is our ability to scrutinise and challenge each and every aspect of the process in a transparent and verifiable way. We trust electoral officials to act honestly, but allow scrutiny by observers when ballots are transported, opened, and counted.

Achieving transparency and verifiability in computerised voting is very difficult, because a person cannot observe directly what a computer is actually doing. A voter interacting with a PC, or a group of scrutineers watching a display screen, cannot actually observe what is happening to the electronic data. Hardware and software errors, accidental configuration errors, or deliberate manipulation or hacking, could all cause privacy to be breached or votes to be modified, misrecorded, dropped or miscounted. Particularly insidious is the fact that all of these could happen without being detected!

Electronic security breaches on important government and financial infrastructure are common. This month the US Democratic National Congress was reportedly compromised by Russian hackers (Nakashima, 2016). Also, it seems about $US55 million was electronically stolen from Ethereum, a flexible blockchain-based network that included both voting and financial functions (Vigna, 2016). Electronic voting systems would not be immune from such attacks. Indeed, Internet voting is harder to secure (for privacy reasons) and has higher stakes than most other Internet applications. The 2015 NSW iVote system contained a serious vulnerability that exposed 66,000 votes to the risk of privacy breach and manipulation. There is neither evidence that it was exploited, nor evidence that it was not.

As the debacle in Western Australia has shown, our paper-based elections are not perfect, but they are certainly open to scrutiny and challenge! The parties involved were able to conclude with confidence that some ballots went missing and that the missing ballots cast enough doubt on the result to make it unacceptable.

The challenge is to use computers while preserving confidence in the election through openness to meaningful scrutiny. A vital question to ask is this: will the electronic vote-casting and vote-counting system withstand a legal challenge in the Court of Disputed Returns? There are two important themes:

Recommendation 1 [Transparency]: *The system's source code and documentation should be publicly available for open review. This is already true for vVote and some of the VEC's other code.*

Recommendation 2 [Verifiability]: *For each election, each voter should get good evidence that their vote is cast in the way that they intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied. E-voting should provide a printout for voters to verify (a voter-verifiable paper trail), or some other form of direct verification (like the vVote system).*

Paper processes are not perfectly secure or reliable, but neither are computers. For example, the lost vote rate in the 2013 West Australian Senate race (1370 out of 1,348,797, slightly over 0.1%) was about the same as the demonstrated vote misrecording rate in Australia's first large Internet voting trial, the 2011 NSW iVote project (43 misrecorded electronic votes out of 46,864, slightly under 0.1%) (PWC, 2011). The WA Senate incident received much more attention because it impacted an election outcome, not because the system was inherently much less reliable. Even more importantly, the paper-based Senate process retained paper evidence of the 99.9% of votes that weren't lost; the iVote system produced no meaningful evidence of the correctness of any of the votes.

We recently discovered an electronic counting error that shifted the winning probabilities in a NSW local government election in 2012 (Conway, 2016). In the council of Griffith, candidate Rina Mercuri narrowly missed out on a seat. We believe the software error incorrectly decreased Mercuri's winning probability to about 10%. According to our count she should have won with 91% probability.

Reliability, privacy and verifiability must be designed into electronic voting processes as carefully as they are designed into our existing paper-based processes. We should ask for verifiable evidence that the election result is correct *without having to trust the software.*

(REMOTE) INTERNET VOTING

The rest of this submission details the verifiability of various options for remote and in-person electronic voting. We focus on evidence that the votes are recorded as the voter intended, transferred securely, and accurately reported.

Secure and usable remote electronic voting, *i.e.* Internet voting, remains an unsolved problem. There are various software products available that claim to provide security and verifiability, but experience in other states, particularly NSW, has shown serious problems relating to reliability, security and verifiability.

IVOTE SECURITY AND VERIFIABILITY

The 2015 run of iVote was implemented by Scytl and run for nearly two weeks in the NSW State Election. During the election, Alex Halderman and Vanessa Teague discovered a serious security problem which would have allowed a network-based attacker to take over the voting session, expose how the person wanted to vote, change the vote before it was submitted, and prevent the voter reading the manipulated vote from the verification server.

The abstract of the paper is included here. The full analysis is available at http://arxiv.org/abs/1504.05646

> *In the world's largest-ever deployment of online voting, the iVote Internet voting system was trusted for the return of 280,000 ballots in the 2015 state election in New South Wales, Australia. During the election, we performed an independent security analysis of parts of the live iVote system and uncovered severe vulnerabilities that could be leveraged to manipulate votes, violate ballot privacy, and subvert the verification mechanism. These vulnerabilities do not seem to have been detected by the election authorities before we disclosed them, despite a pre-election security review and despite the system having run in a live state election for five days. One vulnerability, the result of including analytics software from an insecure external server, exposed some votes to complete compromise of privacy and integrity. At least one parliamentary seat was decided by a margin much smaller than the number of votes taken while the system was vulnerable. We also found protocol flaws, including vote verification that was itself susceptible to manipulation. This incident underscores the difficulty of conducting secure elections online and carries lessons for voters, election officials, and the e-voting research community.*

Approximately 66,000 votes were cast in the days before the security problem was identified and fixed.

The officials at NSWEC at the time took our security analysis as a personal attack, and responded similarly, to the extent that the University of Melbourne was motivated to respond (Zobel, 2015). We would be happy to answer questions about any of that.

In the Legislative Council, some first-preference vote tallies produced by iVote differed notably from those received via paper-based methods. For example, the ALP received more than 30% of the vote from every other method, but only 25% of iVotes. The reason for this discrepancy is unclear. We know of no way to discern whether this was a result of a donkey vote (whatever that means), a user interface problem, a software error, or a security breach involving deliberate vote manipulation.

IVOTE VERIFIABILITY

iVote was not verifiable, despite repeated claims to the contrary. Voters could telephone a verification service, enter their iVote ID and the receipt number they got when they voted, and hear a recorded vote read back to them. There are two main problems with this:

1. Privacy. The verification service could read all the votes. If someone called from an identifiable telephone number, it would be possible to link that person to their vote.

2. Verifiability. There was only a very poorly-described process for a limited number of participants to verify the subsequent vote processing. There are numerous ways to circumvent iVote's verification mechanism, even without access to the central system. We wrote to the NSW electoral commission in 2013 to explain serious weaknesses in the verification protocol, which have never been addressed.

More importantly, almost no information about the actual iVote run in 2015 has yet appeared. In 2011, the 'N' ballot problem was only revealed when PWC's audit report was published. For 2015, the equivalent report remains unavailable.

NSWEC stated that "Some 1.7% of electors who voted using iVote also used the verification service and none of them identified any anomalies with their vote." (NSWEC, 2015) If we consider the total inability to retrieve a vote as an "anomaly", then we do not believe this claim is true. Voters needed to remember a 12-digit receipt number to verify, so it's unlikely they would all have succeeded even if the system had been secure and reliable. But there are other reasons for failure: if votes had been dropped, or if a security problem had been exploited to manipulate votes, we would expect the victims either not to call the correct verification number at all, or to call and find that they couldn't retrieve a vote. So like any kind of audit, the important thing is not the number of successes, but the rate of failure.

The crucial question is,

Of those who tried to verify, what fraction failed?

INTERNET VOTING UNSOLVED PROBLEMS

Recommendation 3 [Internet Voting]: Secure and usable remote electronic voting, i.e. Internet voting, remains an unsolved problem. If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.

The main outstanding technical challenges are:

1) **Cast-as-intended (voter) verifiability**, otherwise known as defence against a compromised client (PC). This means giving each voter evidence that their (electronic) vote matches their intention, and has not been manipulated or misrecorded.

2) **Voter authentication**. This means ensuring that the person casting the vote is the eligible voter they claim to be. Voter authentication is a significant challenge in any kind of voting, but the possibility for large-scale fraud increases when remote electronic options are available.

3) **Verifying the votes are counted as cast and reported or tallied correctly.** This means producing an electronic analogue of the scrutineered paper-handling or paper-counting process in which observers watch the ballot boxes all day, including as they are opened and their contents counted. Some electronic systems produce a paper record for manual counting; others input the electronic vote directly into an electronic count. Either way, they need to prove that the (paper or electronic) vote record matches what the voter cast.

4) **Privacy** is a serious issue, though it is also a serious issue in postal voting. This includes both physical observation of the person voting, and electronic observation of the vote they have cast.

There is considerable research into end-to-end verifiable cryptographic protocols for remote (Internet) voting, mainly addressing the two types of verifiability mentioned as (1) and (3). For example, the Helios voting system (https://vote.heliosvoting.org/) is an open-source implementation of an Internet voting system that includes both cast-as-intended (voter) verifiability and a full mathematical proof that all the votes are counted as cast and tallied correctly. Helios can prove correctness for simple counting algorithms, but would be difficult to extend to preferential elections. At the time of writing no fully verifiable Internet voting system is ready for deployment in real elections. The main reason is that these protocols are very complex and demand considerable work and understanding from voters,

scrutineers and election officials. Furthermore, they do not address issues associated with voter authentication, or all issues associated with privacy or coercion.

Even very simple kinds of fraud could be successfully perpetrated against an Internet voting system. For example, some US political candidates have set up websites apparently soliciting donations for their opponents, but actually keeping the money for their own campaign (Wadhwa, 2014). Similar attacks based on phishing for Internet banking accounts appear in an average inbox almost daily. It would be very difficult to defend an Internet voting application against this sort of simple fraudulent misdirection. Likewise against ordinary distributed denial of service (DDoS) attacks, such as that deployed against an Internet voting system in Canada (Elections BC, 2014).

At present no Internet voting solution exists that provides a degree of security and verifiability as good as postal voting for those who can fill in their own postal vote. For voters who need assistance filling in their paper vote, the verifiable polling-place electronic voting solutions described below provide superior security and verifiability to any Internet voting solution now available, or likely to be available in the near future. Disabled voters' democratic rights are not improved by providing an accessible remote voting solution that does not protect the integrity of their vote as well as alternative methods.

VOTING BY EMAIL (NOT RECOMMENDED)

Voting by email is a particularly insecure form of Internet voting. Although commonly (correctly) understood to present serious problems for privacy, email voting also presents a serious risk to integrity. Email accounts are hacked all the time, and email contents or attachments can be modified at the sender's end, the receiver's end, or in many cases in transit.

ELECTRONIC DELIVERY AND PAPER RETURNS (RECOMMENDED)

We have previously suggested electronic delivery of ballot information and paper (postal) voting returns, especially for local government elections which are otherwise a significant burden on the postal service. The idea would be that voters access their list of candidate and party names online, fill out their ballot at home, and then mail it in. Although this remains subject to some of the same vulnerabilities as postal voting, it at least gives voters the opportunity to verify that they send the vote they intended to send.

In Los Angeles County, voters who have obtained a postal ballot and filled it in at home often come to a polling place and cast it (in a postal-voting envelope) into a special box. This gives them most of the convenience of voting from home and most of the integrity guarantees of voting in a polling place, without any need to queue. This could be combined with electronic delivery of ballot information, and might improve convenience for some postal voters in Australia.

We have an ongoing research project to investigate adding end-to-end verifiability to a system of electronic candidate delivery and postal returns.

Recommendation 4 [Electronic delivery and paper returns]: We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.

IN A POLLING PLACE

In a polling place, a simple paper printout can allow voters to verify that their vote is cast as they intended. This is offered in Tasmania and WA to voters who have difficulty using paper and pencil. The voter attends a polling place and interacts with a computer, which then prints out their vote for insertion into an ordinary ballot box alongside all the other votes. This allows each voter to verify that the printout matches their intentions, then scrutineers observe the counting process just as they observe all the other paper ballots being counted.

The VEC's vVote project is another way to provide verifiable evidence of the correct output, while voters vote by computer in a polling place. The crucial advantage vVote over the "Tasmanian" system above is that there is no need to retain a paper trail at the polling place (or transport a paper trail back to a counting centre) because a full electronic proof is provided to everyone. Hence it is particularly well suited to early and absent attendance voting (*e.g.* in the London High Commission). However, the system is more difficult to administer and use than the simpler "Tasmanian" system, which relies instead on a secured trail of paper votes. Suggestions for improving vVote were included in our prior submission.

In either of those two cases, it would be reasonable to extend eligibility to everyone who wanted to use the system, rather than restricting it to just those voters who would require assistance voting on paper.

If the VEC decided not to rerun vVote in the next state election, they could easily modify the existing open-source software to produce a voter-verifiable paper record instead.

SUMMARY AND CONCLUSION

Despite years of research, nobody knows how to provide evidence of an accurate result while keeping individual Internet votes private. Ask the same questions of an Internet voting system that you would ask of any other way of outsourcing election conduct.

- How are the votes secured against manipulation?
- What if there is an accidental error?
- How do scrutineers get evidence that the result is right?

Receiving votes from the internet is the easy part. Proving that you got the right result, while keeping votes private, is an unsolved problem.

SOME COMMENTS ON THE NATIONAL DEBATE

Policymakers and election officials need an accurate understanding of the technical facts in order to make good decisions. Many software products that purport to increase participation or improve privacy for disadvantaged or overseas voters do no such thing, or do so only at the expense of the integrity of the vote. An accurate technical assessment of the proposed solution, its security, privacy and verifiability, should inform decisions about whether and how widely it should be deployed.

The ultimate test of the verifiability of an electronic voting solution is whether a candidate who disputes an election outcome based on a software system can convince the Court of Disputed Returns that the evidence supporting that system's output is inadequate. A transparent system that provides voters with direct evidence that their votes are cast as they intended, and provides voters or at least scrutineers, with genuine evidence that all the votes are correctly dealt with, is much more likely to stand up to dispute.

BIBLIOGRAPHY

Conway, A. a. (2016, June). *Software Can affect election results.* Retrieved from ElectionWatch: http://electionwatch.unimelb.edu.au/articles/software-can-affect-election-results

Elections BC. (2014). *Recommendations report to the legislative assembly of British Columbia.* Retrieved from http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

Nakashima, E. (2016, June 20). *Cyber researchers confirm Russian government hack of Democratic National Committee.* Retrieved from Washington Post: https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html

NSWEC. (2015). *Response from the NSW Electoral Commission to iVote Security Allegations.* Retrieved from http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports/response_from_the_nsw_electoral_commission_to_ivote_security_allegations

PWC. (2011). *iVote Post-implementation report.* NSW Electoral Commission. Retrieved from http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf

Vigna, P. (2016, June 17). *Fund Based on Digital Currency Ethereum to Wind Down After Alleged Hack.* Retrieved from Wall St Journal:

http://www.wsj.com/articles/investment-fund-based-on-digital-currency-to-wind-down-after-alleged-hack-1466175033

Wadhwa, T. (2014, Jul 2). *Republicans Using Fake Websites To Trick Donors Is Just The Start*. Retrieved from Forbes.com: http://www.forbes.com/sites/tarunwadhwa/2014/02/07/republicans-using-fake-websites-to-trick-donors-and-the-troubling-ethics-of-online-political-campaigns/

Zobel, J. (2015). *Rejoinder To A Statement By The NSW Electoral Commission* . Retrieved from University of Melbourne, Department of Computing and Information Systems: www.cis.unimelb.edu.au/rejoinder/pdf/rejoinder-to-nswec.pdf