SUBMISSION TO PARLIAMENT OF AUSTRALIA JSCEM INQUIRY INTO THE 2016 FEDERAL ELECTION

Dr Chris Culnane and Dr Vanessa Teague
Computing and Information Systems,
University of Melbourne

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

This submission addresses security, privacy, transparency and verifiability of electronic voting and vote counting. Much of this report is identical to our submission to the inquiry into the 2013 federal election. The main arguments and recommendations are the same, but we have updated the examples.

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 did some paid consulting work on electronic vote-counting in 2005. 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 cryptographic protocols, particularly those for verifiable elections and other public processes. She is an Advisory Board member of Verified Voting, a non-partisan non-profit US organization that advocates for legislation and regulation that promotes accuracy, transparency and verifiability of elections.

Dr Chris Culnane is a research fellow also specialising in cryptographic protocols for electronic voting. He was the lead developer, for the University of Surrey, on the Victorian Electoral Commission's vVote project, the first end-to-end verifiable voting system to run at a state level anywhere in the world.

None of the authors have any financial interest in electronic voting.

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

Contents

SUMMARY OF RECOMMENDATIONS:

All these recommendations except the last are identical to those we made in 2013.

Recommendation 1 [Transparency]: *The system's source code and documentation should be publicly available for open review. In particular, we support the request to make the AEC's Senate counting code openly available.*

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 [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. It should be used. It would also be better if the algorithmic approximations introduced for hand counting were removed.*

Recommendation 4 [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 5 [Electronic delivery and paper returns]: *We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.*

Recommendation 6 [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.*

Recommendation 7 [Audit of Senate ballots]: *When the preference data files for Senate votes are published, there should be a rigorous statistical audit to check that they accurately reflect the paper ballots.*

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, their privacy can be violated, or if the system fails to provide evidence that stands up to dispute.

This submission considers three ways of including computers in elections:

1. **Electronic counting of STV votes (p.7),**

   This should be conducted using an open-source counting program, preferably one that has been formally verified to implement the count correctly. There should be a rigorous statistical audit in the presence of scrutineers, to check that the electronic vote data accurately reflect the paper ballots.

2. **Electronic voting in a supervised polling place (p.15),**

   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.

3. **Internet voting (p.9).**

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

Field Code Changed
Formatted: Font: Bold
Formatted: Font: Bold
Field Code Changed

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.

As the debacle in Western Australia has shown, our paper-based elections are not perfect, but they meet the above criterion because 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. However, paper-based elections can be slow to produce results, are becoming increasingly logistically difficult and impinge on the privacy of impaired voters who must be assisted by others to cast their vote. The challenge is to use computers while preserving confidence in the election through openness to meaningful scrutiny.

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!

At the time of writing, the USA is facing a contentious election run partly on e-voting systems that are genuinely insecure and unverifiable. These are typically polling-place computers without a voter-verifiable paper record, but Internet voting is also used in some states. US computer scientists have expressed concerns for many years, resulting in some improvements (such as compulsory auditing of voter-verifiable paper records) in some states, but not all. Daily US election commentary focuses on the risks that the election outcome could be deliberately manipulated. Even if it is not manipulated, the demonstrated fact that those systems are insecure, and the obvious point that they provide no voter-verifiable paper record or other evidence of getting the right result, raise the serious prospect that a US presidential candidate, and many of his supporters, might refuse to accept the election outcome. Even if the election result is correct, the fact that it derives from an unverifiable process is a threat to the stability of US democracy. This is an example Australia should not follow.

In the last few decades, many Australian electoral processes have shifted from manual paper-based processes observed by scrutineers, to electronic processes. Some electronic processes have respected the continuing need for verifiability and genuine scrutiny; others have not.

The challenge is to adapt existing principles of transparency, privacy and verifiability to computerised elections. 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.

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.

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 100 times smaller than the verification failure rate in Australia's

largest Internet voting trial, the NSW iVote project (627 verification failures out of approximately 5000 attempts, about 10%). The WA Senate incident received much more attention because the AEC immediately told the public about the issue, and reran the election. The NSW Electoral Commission does not even seem to have understood the implications of the problem they observed. They announced after the election (March 2015) that "1.7% of electors who voted using iVote® also used the verification service and **none of them identified any anomalies with their vote**." However, a NSWEC official told the NSW JSCEM in August 2016 (NSW, 2016) that 627 voters had tried to verify but failed to retrieve any vote at all. This represents a verification failure rate of about 10%. This rate, extrapolated to all 280,000 iVotes, would have been quite enough to call into question the accuracy of the disputed Legislative Council seat, but the disputing candidate was not aware of the failures at the time.

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. The very fact that a serious verification failure occurred, but was not made known to scrutineers or the public, indicates that the system was not verifiable and could not be effectively scrutinised. Reliability, privacy and verifiability must be designed into electronic voting processes as carefully as they are designed into our existing paper-based processes.

In a polling place, many sensible solutions are available, all involving a human-readable paper record so voters can check that their vote is cast as they intended. Some alternatives and tradeoffs are discussed from p. 16. There are no sufficiently secure, private and verifiable options for Internet voting. This is explained from p. 9. This submission examines both these alternatives with an emphasis on the transparency, verifiability, privacy and security of the possible solutions.

We begin with a discussion of transparency in the form of source code availability. This is particularly relevant for electronic (STV) vote counting, but applies to all other aspects of electronic voting too.

TRANSPARENCY

Transparency of electronic voting systems has become quite controversial in Australia, but it's really very simple: the more scrutiny that can be applied to more details of the software system, the more assurance that it does what it is supposed to do. It is harder to run a transparent electronic process than a transparent paper one, because software is harder to understand and follow than familiar manual procedures.

Computerised voting systems, including their source code, all documentation and reports, and the associated physical security procedures should be available to e-voting

and security experts and the public. Source code availability should be enhanced by enough support for compiling, running and understanding the system. This level of transparency should be an enforced condition of the initial tender and contract.

Making a system's source code public does not automatically make it secure or correct. However, neither does keeping its source code secret. Transparency is good for security, because bugs and security vulnerabilities have a better chance of being identified and patched before the election. Having the open source available to the community for technical review by a range of interested experts will increase transparency and trustworthiness of the electronic voting and counting process, because it facilitates an open and scientifically informed discussion about the merits of a proposed system. It also helps find bugs.

The reason this issue is so contentious is that the business interests of software vendors differ from the transparency requirements of election administration. A vendor's priority is its commercial interest. Its obligations are to protect the value of the IP related to its product and also the value of its reputation (obviously it's bad for business if failures, vulnerabilities and shortcomings come to light).

Internationally, some countries continue to use closed-source Internet voting systems. Others, such as Norway, have been open-source all along, while others, such as Estonia, have made their systems open following public pressure[1].

"Auditing" or "certification" by third parties is not a substitute for electoral transparency. Auditing firms do not have the same incentives as candidate-appointed scrutineers. The history of electronic voting "certification" and "auditing", both in Australia and overseas, has produced "certification" reports for systems that actually had serious security vulnerabilities or software errors, including the NSWEC iVote system (PWC, 2011), the VEC 2007 Scytl system[2] (Teague, 2011), (Scytl Secure Electronic Voting, 2011), and the systems by Diebold, Hart and Sequoia analysed in the California Top to Bottom Review. The iVote example and the California Top to bottom review are discussed more below.

STV COUNTING

Australian elections invariably use some form of preferential voting where voters are asked to order a list of candidates by numbering the candidates in order of the voter's preference. Counting such ballots by hand is a notoriously difficult task, especially for STV. Consequently, more and more electoral commissions are turning to computers to count the ballots, whether they be cast electronically or via paper. This raises the question of whether

[1] The Estonian source code is available at https://github.com/vvk-ehk/evalimine

[2] The most serious issue, identified by V Teague, was patched before the election.

the computer program that counts the ballots does so correctly. As demonstrated by the WA election, tens of votes out of millions can make a difference to the end result. Thus interested parties are highly likely to challenge a result that is close.

For example, the Logic and Computation Group at the ANU have found three bugs in the vote-counting module of EVACS, the ACT's open-source electronic voting and counting system. All have been acknowledged by the ACTEC (Elections ACT). Two of them were found by scrutinising the code, but a third was found by running a counting program developed independently by ANU researchers, and tracing the differences in the scrutiny sheets produced by the official program and this ANU program (Dawson, Goré, & Slater, 2003). Each of these bugs could have changed the outcome of the election. Fortunately, none of them manifested themselves in the five elections that have used EVACS: 2001, 2002, 2004, 2008 and 2013. This illustrates several points:

1. ``quality certification'' is meaningless because the code had been "audited" by a commercial quality assurance company, BMM Australia;
2. serious bugs can lie undetected for years;
3. fixing the bugs does not guarantee anything since there may well be other bugs.

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. The NSWEC corrected this error in time for the 2016 local government elections, but two more coding errors manifested in the 2016 count.

We believe the Australian Electoral Commission would benefit greatly in the long term from making its STV (Senate) counting source code publicly available, as requested under the Freedom of Information Act last year (Cordover, 2013). Although the (probable) discovery of some errors might be temporarily embarrassing, in the long term transparency improves the chances of announcing a correct and defensible Senate outcome.

The Victorian Electoral Commission and ACT Electoral Commission have both made their STV counting source code open[3]. Several independent open-source implementations of Senate counting exist, for instance one by Andrew Conway[4] and one by Grahame Bowland[5].

---

[3] The VEC's is at https://www.vec.vic.gov.au/Vote/vote-VEC-ems.html, under "Computerised vote counting"; the ACTEC's at http://www.elections.act.gov.au/__data/assets/file/0004/8185/evacs2012.zip

[4] https://github.com/SiliconEconometrics/PublicService

[5] http://blog.angrygoats.net/2014/01/25/counting-the-west-australian-senate-election/

These allow independent parties to redo the Senate count. So far they have found no discrepancies, but that is no guarantee that either their code or the AEC's is correct.

FORMALLY VERIFIED VOTE-COUNTING PROGRAMS

Modern software verification techniques are now capable of formally verifying that a moderately large computer program does what it is supposed to do. Thus it is perfectly feasible to formally verify that the vote-counting program does indeed count the votes correctly according to the intended STV method.

Recommendation 3 [Counting algorithm verification]: *formal verification that the computer code for vote-counting correctly implements the count is also possible using modern software verification techniques. It should be used. It would also be better if the algorithmic approximations introduced for hand counting were removed.*

Although Senate votes are now counted by computer, legislation retains many simplifying approximations that were intended to make hand counting easier. The method of computing weighted transfer values is one example. These make the code more complicated and harder to verify. Goré *et al.* have recently shown that the presence or absence of these simplifications can alter the result of an election. If we are going to use computers to count the ballots, then simpler methods closer to the original STV algorithm can be implemented since the previous simplifications are just not needed any more.

Of course, none of this obviates the need for scrutineers to be able to check that the paper votes cast by voters match the electronic records entered into the STV count. This is the topic of the next section.

AUDITING THE ACCURACY OF THE SENATE BALLOT DIGITISATION

This year for the first time many Australians expressed their own second or third preferences above the line. This allowed a more expressive vote, which is a good thing, but it also meant that the task of performing and scrutinising the Senate count became more complicated. All the questions about accuracy, transparency and security apply to the electronic scanning and digitising process too.

Automating the scanning and counting of Senate votes is a good idea. However, we need to update our notion of "scrutiny" when so much of the process is electronic. The AEC has implemented some mechanisms for detecting accidental operator or software errors, but these do not constitute complete evidence of an accurate result. For example, there is no verification that the electronic vote records accurately represent what was produced by the automatic recognition or the manual operator, nor that it was the same thing displayed to scrutineers on the screen. It is not comforting that at least some of this process relied on

software from the same company that produced iVote, for which there was a 10% verification failure rate not made public at the time.

This process must be made amenable to meaningful scrutineering by incorporating a rigorous statistical audit of the paper ballots, to ensure that they match the published electronic vote preferences. Specific suggestions for performing the audits are contained in our paper: https://arxiv.org/abs/1610.00127

Recommendation 7 [Audit of Senate ballots]: *When the preference data files for Senate votes are published, there should be a rigorous statistical audit to check that they accurately reflect the paper ballots.*

(REMOTE) INTERNET VOTING

The rest of this submission details the verifiability of various options for remote and in-person electronic voting. Everything already said about electronic counting applies here as well, but from now on 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. Most computer scientists recommend strongly against returning voted ballots over the Internet at present.

In contrast to supervised voting in polling places, which enforces secrecy on everyone without requiring them to assert their right to it, remote voting delegates the provision of secrecy to the voter themselves. Internet voting makes the challenge even harder, requiring the voter to not only secure the environment in which they cast their vote, but also to secure the computer and internet connection they will use for voting.

Recommendation 4 [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 challenges are:

> **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.

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.

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.

If the votes are counted electronically, ensuring that the tallying program is itself correct is a major unresolved issue, as described above.

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.

Coercion of voters is a serious concern with any remote voting solution, be it postal or internet. Internet voting enables coercion to be performed more easily at a larger scale. Coercion would not necessarily be detectable or frequently reported. Like other security properties, the coercion-resistance of an Internet voting protocol is difficult to assess – the iVote protocol was claimed to resist coercion by allowing revoting, but its defence does not work (McKay, 2016).

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.

There have been numerous recent news stories about deliberate attacks on the infrastructure of US elections, including voter registration databases. An Internet voting system must be able to withstand that sort of attack, or at least guarantee that it will become evident.

Australia's largest-ever Internet voting trial was the NSW iVote project. The next section examines its security problems and its 10% rate of verification failure.

IVOTE SECURITY AND VERIFIABILITY

The 2015 iVote system 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.

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 iVote administrators and vendor do not seem to have understood an important indication of a possibly serious problem. At the time of the election, the NSW website 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). In hearings at the NSW JSCEM in August 2016, an official said that there were 7 voters who pressed the button to indicate that their vote was not as they intended, of whom 2 subsequently said they had done so by mistake. That leaves 5. When the same official was asked, "Of those who called the verification service, how many failed to retrieve any vote?" he explained that, "627 callers to the verification service out of a total of 5,300 calls had entered their credentials wrongly in some way." That represents a 10% verification failure rate – if that failure rate is extrapolated to all 280,000 iVotes it is more than enough to have changed the outcome of the disputed Legislative Council seat. There is no way to tell whether those failures are the result of voter error, software error, or deliberate manipulation.

All we can say with confidence is that the system is not verifiable. Not only the high failure rate, but the delay of notification until more than a year after the election, indicate that this system is not appropriate for government elections. Even now, there is no independent way to test whether those 627 failures are the true total. PWC's audit report, recently published online by NSWEC (PWC, 2015), refers to an incident described as "fix signature file, which was preventing verification." It is not clear how many verifications were prevented, or whether those failures were included in the 627 failures already reported.

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 is also 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. It might be possible to add some cryptographic techniques for verifying that the vote was accurately received – this is a topic of ongoing research.

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.

Recommendation 5 [Electronic delivery and paper returns]: We should consider alternative methods of using the Internet without necessarily trusting it alone to carry completed ballots.

POLLING-PLACE ELECTRONIC VOTING

Are computers secure as long as they are disconnected from the Internet? The simple answer is no. Although the opportunities for remote attack are reduced, significant opportunities for privacy invasion and vote manipulation could remain. Fortunately, elections conducted in a supervised polling place can be verifiable and reasonably private, while taking advantage of the assistance of computers. Voters should have the opportunity to verify a human-readable paper record of their vote, then the rest of the process should let scrutineers (or the voters themselves) verify that all votes are correctly transported and reported.

Recommendation 6 [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.

It is not enough to test the software or hardware before the election. The system should be designed to provide direct evidence of a correct election outcome.

SECURITY ISSUES THAT REMAIN, EVEN WHEN THE COMPUTER IS DISCONNECTED FROM THE INTERNET

When computerised elections became common in the US after 2000, they were often standalone machines, disconnected from the Internet. Many produced all-electronic election records without a paper backup. Concerns from US computer scientists motivated the authorities in California to conduct a "top-to-bottom" review in 2007 of the security of the main brands of machines that had until then been used in California (California Secretary of State, 2007). The analysis team successfully compromised all of the machines they studied, in ways that could have led to undetectable electoral manipulation if they had been perpetrated in a real election. One team wrote:

"The testers discovered numerous ways to overwrite the firmware of the Sequoia Edge system, ..., the attackers controlled the machine, and could manipulate the results of the election."

These insecure systems had already been "certified" by an "independent" testing lab. However, in the light of the Top-to-bottom review, they were decertified. Californian legislation now requires all electronic voting machines to produce a voter-verifiable paper record for auditing or manual counting.

Polling place electronic voting machines were purchased for Ireland and then never used, after security researchers demonstrated serious privacy and integrity flaws. The total cost of buying, storing and scrapping the machines was more than €50 million.

Although the ACT's EVACS voting system set a laudable standard for transparency when (at least some parts of) its source code was made available, its design does not adequately defend against attacks on the machines themselves. Indeed it seems to have been designed with the assumption that it does not need to address security problems because it is not connected to the Internet. However, many people have significant access to the machines before and during the voting period, so the same kinds of attacks identified in the California top to bottom review could quite possibly apply. Attacks on the firmware or BIOS could remain undetected even when the computer is supposed to boot from another source (Butterworth, 2013).

The following section describes two methods of providing verifiable election outcomes. Both use a human-readable vote printout.

VERIFIABLE POLLING-PLACE ELECTRONIC VOTING

Computer-assisted voting in a polling place is a solved problem with several sensible solutions. They all involve a human-readable paper record, which the voter can check to see that their vote is cast as they intended.

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.

"Verifiability" needs to be made precise in order to be meaningful. Many electronic voting software vendors advertise "verifiable" products which in fact provide very little meaningful evidence of having achieved the correct result. Some examples of genuinely verifiable solutions are given below:

- **Computer-assisted attendance voting with a human-readable paper trail.** The voter 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. This simple and voter-verifiable solution is offered in Tasmania and WA to voters who have difficulty using paper and pencil.

Several other election authorities, particularly in the USA, use a combination of electronic assistance and a voter-verifiable paper record. Variants include optically scanned paper ballots, electronic voting with a voter-verifiable paper audit trail

(VVPAT), and a few others. The unifying theme is that the voter can see a permanent paper record of their vote, which is retained as evidence.

The VEC's end-to-end verifiable attendance voting project, based on prêt à voter. This system uses complex cryptography to provide each voter with good evidence that their votes are cast in the way that they intended, and included unmodified in the count, and a public mathematical proof that all the votes (from this system) are accurately output. Voters verify a printout of their vote, and then take home a receipt, which does not prove how they voted, but can be used later to check that their vote has been included without modification. Culnane was the lead developer on this project; Teague has been working on it on a voluntary basis.

The crucial advantage of prêt à voter 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. 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. It remains to be seen whether the increased complexity of this system is tolerable for voters, scrutineers or electoral officials. In either of those two cases, eligibility could extend to everyone who wanted to use the system, rather than restricting it to just those voters who would require assistance voting on paper. It would also be reasonable to run these systems for ADF personnel or overseas Australians, in a temporary but supervised polling place such as that run by the VEC in the Australian High Commission in London.

SUMMARY AND CONCLUSION

The most secure way to vote is in a supervised polling place. A computer in a polling place can help prevent accidental informal voting, and help voters with disabilities to vote independently. However, the system must provide a human-readable paper record so that the voter can check that their vote is cast as they intended (Recommendation 6). This record should be linked to a method allowing scrutineers or voters to check that the record is included unaltered in the count (Recommendation 2). This could be achieved by plain paper or by an end-to-end verifiable voting system like Victoria's vVote system.

It's important to realise that a "polling place" need not necessarily be a permanent one, and that temporary kiosk-style polling places with verifiable electronic voting systems could be one good solution for overseas or ADF personnel.

There are few good solutions for remote voters, and no good solutions for returning voted ballots over the internet (Recommendation 4). It is worth considering sending out blank ballots via the internet and returning a filled-in paper ballot (Recommendation 5).

For either kind of system, the system's source code and documents should be openly available (Recommendation 1). For electronic STV counting especially, the software could benefit greatly from formal verification of its correctness if made publicly available (Recommendation 3). The electronic Senate vote records should be audited, in the presence of scrutineers, against the paper evidence of how people voted (Recommendation 7).

If a polling-place electronic voting system provides direct verification that the voter's vote was captured as intended as outlined in Recommendation 6, and evidence of correct inclusion (Recommendation 2), and if the STV votes are counted correctly with an open-source formally verified vote-counting program (Recommendations 1 and 3), then it is very difficult to argue against their result in a court of disputed returns.

BIBLIOGRAPHY

Butterworth, J. (2013). Bios chronomancy: Fixing the core root of trust for measurement. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.* ACM.

California Secretary of State. (2007). *California top to bottom review of voting*. Retrieved from http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

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

Cordover, M. (2013, Oct). *righttoknow.org*. Retrieved from https://www.righttoknow.org.au/request/software_by_which_senate_counts

Dawson, J., Goré, R., & Slater, A. (2003). *Formal Methods Applied to Electronic Voting Systems*. Retrieved from http://users.cecs.anu.edu.au/~rpg/EVoting/

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

Electoral Council of Australia and New Zealand. (2013). Internet voting in Australian election systems. Retrieved from http://www.eca.gov.au/research/files/internet-voting-australian-election-systems.pdf

Estonian National Electoral Committee. (n.d.). Retrieved from http://www.vvk.ee/voting-methods-in-estonia/engindex/

Jefferson, D. (n.d.). Retrieved from VerifiedVoting.org: https://www.verifiedvoting.org/resources/internet-voting/vote-online/

McKay, R. (2016). Submission to the Victorian Electoral Matters Committee Inquiry into Electronic Voting. Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/emc/Inquiry_into_Electronic_Voting/Submissions/No_29_Ralph_McKay.pdf

NSW Electoral Commission. (n.d.). *iVote Approved Procedures for 2011 NSW State General Election, 4.8.2(3)*. Retrieved from https://www.elections.nsw.gov.au/publications/policies/ivote_approved_procedures/4._approved_procedures/4.8_authentication_of_vote

NSW, P. o. (2016). Hearings before the Joint Standing Committee on Electoral Matters Inquiry into the conduct of the 2015 state election. Retrieved from https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryEventTranscript/Transcript/9731/Hearing%20Transcript.PDF

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

OSCE/ODIHR. (2011). *Estonia Parliamentary elections OSCE/ODIHR election assessment mission report.* Organisation for security and cooperation in Europe, Office for Democratic institutions and human rights. Retrieved from http://www.osce.org/odihr/77557

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

PWC. (2015). *Post-implementation review of the iVote project.* Retrieved from http://www.elections.nsw.gov.au/__data/assets/pdf_file/0020/220484/NSWEC_iVote_Post-Implementation_Report_FINAL.pdf

Scytl Secure Electronic Voting. (2011). *Comments from Scytl on the CORE report from the electronic voting solution used in the 2010 Victorian Election.* Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/14_Scytl_EMC_Inquiry_No.6.pdf

Teague, V. (2011). *CORE Submission to the Victorian Parliamentary Inquiry into the conduct of the 2010 Victorian State election.* Retrieved from http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/13_VTeague_EMC_Inquiry_No.6.pdf

Teague, V., & Wen, R. (2012, Feb). *CORE Submission to the inquiry into the administration of the 2011 NSW State Election.* Retrieved from http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/ba09355ede5e3859ca2579ad0001d53c/$FILE/Submission%207%20-%20Core.pdf

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/

Zheng, Y. (2014, Feb 13). *The Oregonian.* Retrieved from http://www.oregonlive.com/politics/index.ssf/2014/02/frustrations_mount_as_oregon_s.html