Verifiable Electronic Voting in Practice: the use of vVote in the Victorian State Election

Craig Burton[1], Chris Culnane[2] and Steve Schneider[2]
[1] formerly Victorian Electoral Commission, Victoria, Australia
[2] University of Surrey, UK

November 2, 2015

Keywords: Voting/election technologies; Security protocols; Domain-specific security and privacy architectures; Usability in security and privacy; Software security engineering

1 Introduction

Proposals for verifiable electronic voting that provide assurances for secrecy of the ballot and integrity of the election have been in the academic literature since the early 1980s with real world systems proposed in the 2000's — but the challenge of making verifiable voting usable and practical for ordinary voters and integration into existing paper based election processes has meant that practical deployment has been slow in coming.

This paper reports on the experience of deploying the vVote verifiable voting system in the November 2014 State election in Victoria, Australia. It describes the system that was deployed, discusses its end-to-end verifiability, and reports on the voters and poll workers experience with the system.

The State of Victoria has a proud history of innovation in voting systems, having introduced the first strict supervisory controls at polling places in 1856 [1] with government printed ballots, logistic checks and balances and the private booth. More recently, the Victorian Electoral Commission (VEC) was an early adopter of electronic voting, and fielded systems in 2006 and 2010. The Electoral Act changes for electronic voting in Victoria intended better accessibility for blind, partially sighted, and motor impaired voters through customised computer voting interfaces. The Act was amended in 2010 to extend access to voters speaking languages other than English and any voters out of state and overseas, enabling more rapid return of the votes into the tallying process.

Australia has no e-voting standards or guidelines (except the voluntary Telephone Voting Standards TVS2.0) so the Victorian Electoral Commission was guided by the US Voluntary Voting System Guidelines [2] as these were seen to be the most recent, progressive, and considered networked IT security threats. In addition *software independence* [3] is a critical basis for trustworthy voting systems: that "an undetected change or error in the software cannot cause an undetectable change or error in the election outcome". In place of systems certification, an e-voting specialist agency Demtech, was selected to review compliance with the published protocols and fitness to deploy [4].

The election system in Victoria poses particular challenges for any verifiable solution, because of the complexity of the ballots. Voters vote in two races in State Elections: for the Legislative Assembly, voters rank all of the candidates in preferential order, usually up to ten candidates. For the Legislative Council voters either select one party or group (Above Line), or they rank the individual candidates (typically up to 40) in their preferred order (Below Line).

There are 8 regions comprising 88 districts, so there are 96 races in total. Nominations for candidates

were open until Noon on Friday 14th November 2014, and the electronic system needed to be ready to take votes from Monday 17th November. There is a period of two weeks of "early voting" for which the electronic system is deployed, up to the official election day on Saturday 29th November. Electronic voting is only available during early voting and voters are allowed to use any polling station to cast a ballot in their home races. Thus all polling stations must offer ballot forms for all the races across the State.

The total number of registered voters for the 2014 election was 3.8 million, of whom the Australian Bureau of Statistics[1] indicate as many as 186,000 Victorian travellers, 100,000 adults not proficient in English and 118,000 adults with low vision or blindness[2] were eligible to vote using the electronic system.

A total of 1121 votes were collected. This was more votes than were collected by the 2010 electronic system, and the system was deployed at fewer locations (25 instead of 101).

2 Related work

The only statutory end-to-end verifiable elections to date have taken place in Takoma Park, Maryland, US, where the Scantegrity system was successfully used in 2009 and 2011 in the municipal election for mayor and city council members [5]. Scantegrity has been adapted and trialled for remote voting ("Remotegrity") [6] as well as voting for blind voters ("Audiotegrity") [7]. This groundbreaking work demonstrated the feasibility of running an election in a verifiable way, including with people who have barriers to voting. However, the Scantegrity system becomes impractical with a preferential ballot of up to 40 candidates and may require up to 200 mark-sense ovals to allow ordering of at least 5 candidates in this case and many more to allow numbering all 40 candidates in order of preference.

There is a rich body of work covering remote voting, DRE machines and many others which we cannot summarise here. We were specifically pursuing end-to-end verifiability (E2EV) at scale and as such this is the first work of its kind. We direct the reader to [8] for an introduction to verifiability in electronic voting systems, and to [9] for coverage of related systems.

E2EV is an approach to computer security designed specifically for elections, which provides highly reliable detection of loss, damage or fraud affecting votes. It is not a method of defence but it does provide an important new deterrent because any attacker has to consider the likelihood of detection. It is the case many current security systems can only report the attacks they have detected. E2EV detects, with high probability, attempts to change the election outcome, whether the voting system software performs as expected or not — this is software independence. vVote was created to safely collect votes in a verifiable manner and it replaced a previous third party system that was not end-to-end verifiable.

3 System Description

The starting point for the design of vVote was the Prêt à Voter split ballot [10] in Figure 1. Since paper-based Prêt à Voter has had differing usability assessment results in its paper form [11, 12], considerable work went in to its electronic form. It was mandated that accessibility must extend to polling place verification. The completed technical design of the system as deployed is described in [13], where comparisons with other electronic voting schemes are also discussed.

To facilitate electronic capture, an Electronic Ballot Marker (EBM) was introduced: a common tablet computer (Google Nexus 10) that provided a voter interface for capturing the vote. The ballot forms needed to be printed on demand on a separate tablet of the same make called the vVote Printing Server (VPS) for use in each polling place. The design also introduced a distributed Web Bulletin Board (WBB) for accepting the votes and making information public and immutable.

Once a voter is marked off the electoral roll, they are printed a candidate list (CL) with the names in a random order. Voters can demand that their CL is

[1] http://www.abs.gov.au/ausstats

[2] Blind Citizens Australia, Australian Blind and Vision Impaired Statistics

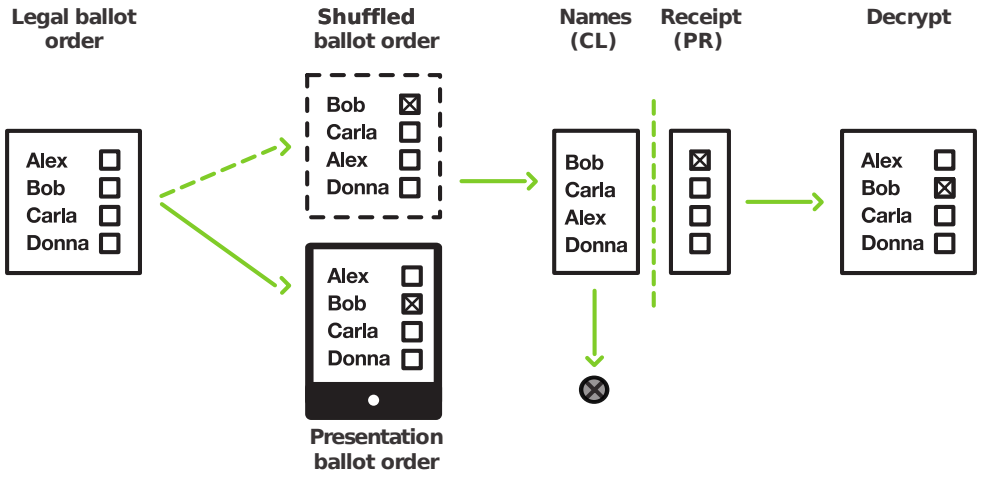


Figure 1: Prêt à Voter with an EBM: The legal ballot order (at left) is shuffled to create candidate lists (CL). The presentation order in paper Prêt à Voter is shuffled (top ballots). The vVote ballot (shown on an EBM) is the legal order. The tablet reads the CL and on receiving the vote it produces the preferences receipt (PR) in the shuffled order. The CL is destroyed after matching against the PR. The PR is retained by the voter. The information from the PR is later passed through an anonymising mixnet and then decrypted to reveal the legal order needed for counting.

'audited' to check that the printed order matches the encrypted order that the system has already committed to. An audited CL cannot then be used to vote and all such audit results are made public automatically. Following audit the voter is issued with a new CL. In the 2014 deployment voters were *not* alerted to this possibility since there was a concern that the subtlety of what it was achieving (essentially random sampling of correct construction of the ballot forms) was too complex for voters to absorb on the spot or may cause delays and queueing. For future deployments some advance education would raise awareness of this step. The effects of this on verifiability are discussed below.

When the voter uses a CL to vote, it is read by an external camera attached to the tablet. The booth setup for blind voters is illustrated in Figure 2(1) which shows a tablet computer with a latex screen overlay that functions like a phone keypad. Another interface also for blind voters provided the unlit screen as a swiping surface. Scanning of the candidate list QR code launches the vote capture application, which allows the voter to enter their vote. The EBM interface for sighted voters is illustrated in Figure 2(2–5). Having voted, a preferences receipt (PR) is printed separately. The voter verifies that the preferences match the correct candidate names, by comparing the lists side by side, as in Figure 2(6) (or via audio means as below). This check ensures that the receipt captures the vote as cast. Once this is done the CL must be destroyed in order to keep the vote secret. The PR is retained by the voter. The fact that the candidate names were in a shuffled order ensures that the PR does not expose who the preferences were for and thus provides ballot secrecy.

The system allows staff to 'quarantine' or cancel a vote if the PR is not provided for any reason, or if the voter considers it to be incorrect, and in such cases where the voter reports serious usability issues. The voter must furnish their CL to request this. Looking up a serial number for a quarantined vote results in the WBB reporting a signed transaction so this cannot occur silently. Another kind of quarantine is called Bulk Quarantine and is a mechanism where by

the electoral commission can exclude all votes from one device from being decrypted. Bulk quarantine occurs *outside the protocol* and is considered a manual intervention. In the deployment there were 6 individual quarantines (due to a receipt printing problem) and one bulk quarantine (of a single vote, due to a usability problem and a lost CL).

The voter later looks up their PR on the WBB, and verifies that it has been included properly, or can raise a challenge if not. At any time the voter (or anyone) can also examine the QR code on the PR to see or hear the shuffled order of their preferences, which should match the visual display. An Android phone app was also developed that checks the PR signature against the public key for the election to confirm the central recording system signed the return. This was available but not promoted.

It is important to add that all aspects of the voting ceremony as well as the verification measures intended for voters were also made accessible. A ballot audit could be taken to an EBM and the device would read the contents out. Both the CL and PR could be read out separately on any EBM or if provided together (to give the shuffled order of candidate names if required), the assembled preference-order vote could be read back to the voter.

Voters can check that their vote is *cast as intended* via the CL-PR check. They confirm their vote is *recorded as cast* by checking that their preferences on the receipt correspond to the information recorded on the WBB. Finally, it is publicly verifiable that the correct tally is returned, *counted as recorded*, because the mixing and decrypting of the encrypted votes generates cryptographic proofs that can be independently checked. This provides a chain of links all the way from the initial creation of blank ballots to casting of the vote right through to the tallying.

In this election the electronic votes needed to be combined with paper votes, and so the electronic votes were printed off to be included within the paper count. Each printed vote paper included as a footer the line number for that preference data in the decrypted, emitted CSV files of raw votes for staff spot-audits. In this case we have verifiability through to the decrypted votes: that any cast vote made it into the paper count, which was then done in the usual way.

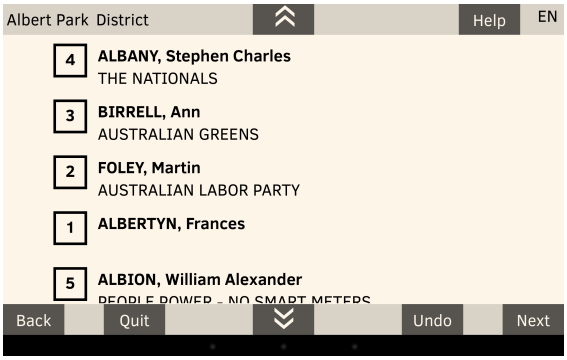
4 Staff training and voter support

Concepts in E2EV are very new and some are inconsistent with paper election procedures. For example, the presence of E2EV ballot audits as an *option* the voter can pursue is not consistent with conventional security practices such as seals, which must *all* be used, checked, documented and inspected. The nexus between the simple act of depositing a paper ballot (irretrievably) from a ballot box and the highly complex nature of transmission and storage of an e-vote to its repository made 'quarantine' a necessary mitigation. The paper voting system also has a concept of quarantine of votes (such as provisional votes for those voters not found on the electoral register), but this does not allow removal of a vote from the ballot box.

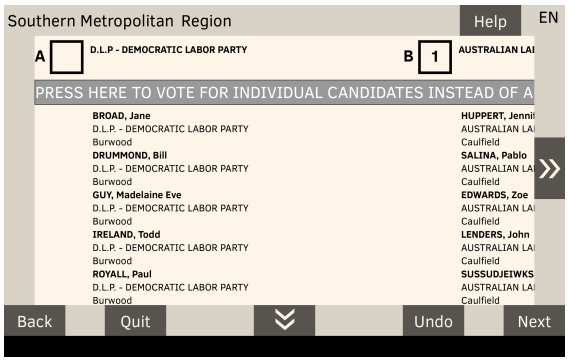
vVote follows paper voting logistic processes more closely than previous e-voting systems used by VEC. For example, vVote creates fixed numbers of blank ballots in advance of the election. Previous systems "created" ballots as they needed them, potentially an uncontrollable quantity. Despite similarities, some new concepts such as the random permutation of candidates also made training more difficult. Trainees as well as the executive were not certain how many questions voters would ask and how to answer them quickly whilst not obscuring transparency aspects of the system design. It is likely that longer term E2EV will settle in the public consciousness the same way that Single Transferrable Vote (STV) counting is accepted but not actually fully understood by most Australians. Low STV comprehension may be lamentable but in fact those who do not understand it trust that ample others observe and enforce that STV is performed correctly. We hope this situation evolves for E2EV.

During development, iterations of the system were tested under controlled conditions and the same verbal instruction given to cohorts of target users who were provided to VEC via disability organisations

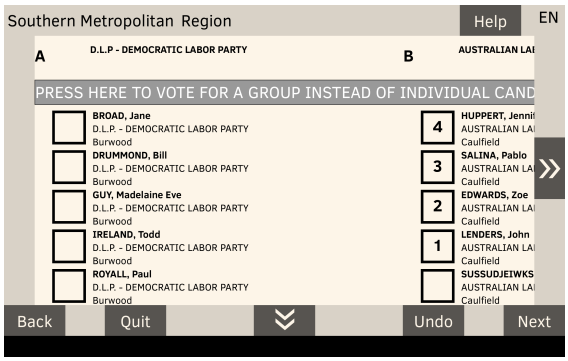
1. A voting booth for use by blind voters. A tactile latex 'telephone keypad' overlay sits on the touchscreen, and headphones provide audio instructions.



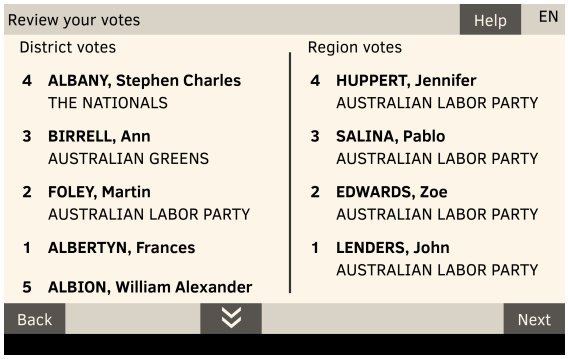
2. District ballot visual interface showing preferences assigned. Voter must number all candidates. Double arrow scrolls the ballot.



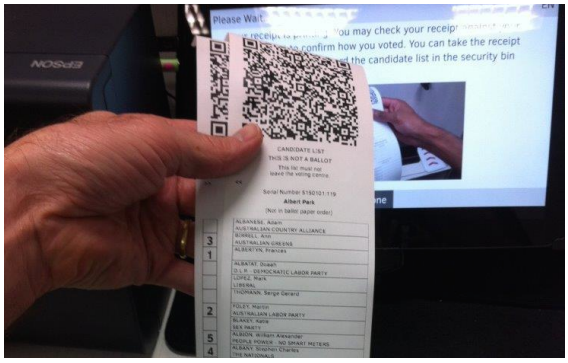
3. Region ballot showing required Above Line preference assigned. Voter must choose one party or group.



4. Region ballot showing Below Line preferences assigned. Voter must number 5 or more candidates.



5. Summary of preferences for both races in legal ballot order.



6. Visual matching of the candidate list (CL) and preference receipt (PR).

Figure 2: Physical and graphic interfaces

and community groups. In all more than 150 people were videotaped using the system at least once and the system was modified to log interface events (this was removed before the live election). The cohorts were: functionally blind users (8); users with a range of low-vision types including retinopathy and tunnel vision (10); non-English speaking Arabic (8) and Mandarin speakers (10); able-bodied English speakers (including VEC sessional and permanent staff of more than 100); and five subjects who were profoundly disabled with normal cognitive function and vision.

Much was learned from this process and many changes to the system were re-tested. Experiences with right-to-left language di-plurals, drag-and-drop preference renumbering and a CL that was physically torn from its PR are some of many trials that led to the current system. Perhaps the most interesting observation was that the system was found to be not usable by some non-English speakers because candidate and party names were all voiced and displayed in English. It has been a common assumption that even non-English speakers could pattern match popular party names even if they were not in first languages or that they could transpose advised voting preferences from the party literature (called a How To Vote Card — HTVC) given out on arrival at all polling places. Under testing for the first time with non-bilinguals, Arabic speaking subjects could not for example, find and vote GREENS even with an Arabic language HTVC. In this case, a change request was raised and the system was modified so that touching any (still in English) party name would display and say that name in the best available translation for that language.

Close to the final iteration of the testing, the system was handed over for third party review to Inclusive UX, a Sydney usability firm who had previously assessed electronic voting interfaces in Australia. Inclusive UX did not have a remit to perform their own testing due to time constraints, but were given a fully working system and requested to identify risks in the as-built design. Feedback from this final assessment resulted in changes to coloration (such as removal of graded backgrounds) and audio voting changes (such as fully stating where the audio cursor is on the LC ballot candidate grid).

5 Deployment

Because this was a completely novel system and to limit the cohort requiring additional training, VEC rolled out in a limited deployment in 24 early voting centres around Victoria including 6 "accessibility super centres". It was also deployed in the Australia Centre, London, UK in order to gain experience of the remote voting solution with voters who had no barriers to voting. The London centre was run in the same manner as Victorian centres.

The total number of votes that were received over the two weeks was 1121, of which 973 were from London and the remaining 148 from the 24 centres in the State of Victoria.

In fact the system was developed for much higher demands in order to scale up for future elections: it handled 1 million votes in testing, and under stress was able to respond to individual voters within 10s, and to accept 800 votes in a 10s period.

6 Outcomes

A range of instruments were used to obtain feedback on this project. Participant numbers were small and so the results are indicative and suggest issues for deeper investigation. A University of Surrey survey which intercepted 45 voters leaving the Australia Centre in London having cast their votes is most indicative of the system with the entire voter cohort. For Victoria, VEC collected 29 responses to an anonymous opt-in online questionnaire of 54 poll workers which asked questions about equipment setup and voter support. Both surveys asked about verifiability, trust and security taken from the survey instrument of Karayumak et al [14]. VEC also ran a separate opt-in survey for London voters who volunteered their email addresses (60 responses) as well as for Victorian voters (< 10 responses).

To analyse time-to-vote, server logs were used. Google Analytics collected information for public-facing information and lookup services (not the vot-

ing system). It should also be noted that the voting protocol does not capture voting interface navigation actions (as it allows no metadata) and that the EBM is stateless. These privacy controls prevented live usability data being captured such as the navigation, changing language or undoing vote choices.

It is likely that two technical problems affected survey results. There was a missing instruction in the setup manual for poll workers for when the system went from a training mode to the live voting mode. This absence of this setup step caused the receipt printer not to work until setup was completed properly. Almost all sites were affected by this but early intervention by the VEC help desk and four site visits meant very few voters were affected and the problem was resolved the first day of voting. A second problem was unrelated to vVote and concerned network problems at VEC. This constrained bandwidth and caused some remote sites (including London) to not receive their (29MB) configuration file. Three sites were not online at start of voting. This problem was largely resolved by the second day of voting but London had to revert to paper ballots for two whole days in total. Setup problems in Victoria may have impacted the few voters who attended several sites, causing a disproportionate problem.

Voter surveys

Voters were generally satisfied with the usability of the system, but there was a wide variation in understanding of the security assurances provided. For example, some voters answered that the receipt showed their vote (which it does not, since a receipt should never link directly to any vote). The results are shown in Figure 3. Although most voters trusted the system implicitly they nonetheless took part in the verifiability steps and many said they would check receipts at home — there was no resistance to such new steps reported by Karayumak et al. Data collected in Victoria are for very low numbers of voters and so we focus on the London results for our general findings. It is certainly the case that more work is needed to accurately measure E2EV in the live polling place for both staff and voters, including expectations, error coping and comprehension.

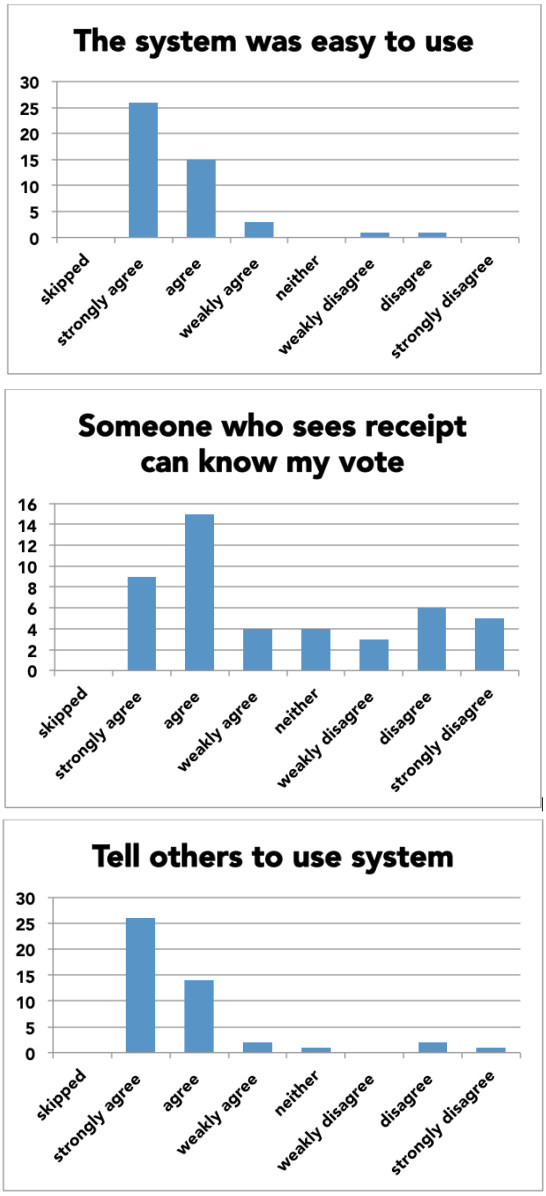


Figure 3: Three questionnaire responses from London

In more detail, the headline results from the **voter surveys** were as follows:

1. Respondents found the system easy to use, as illustrated in Figure 3. 75% or greater respondents stated Agree or Strongly Agree to all positive aspects of usability. 75% stated they preferred the system to paper voting. This is also evident in comments and in the time taken to vote. 60% of respondents voted in 4 minutes or under, with 96% in 5-10 minutes or less. This was the whole time to vote on the system (not the time to get a PR or wait in queues). None stated the process took "too long". 87% stated Agree or Strongly Agree to the statement "I would tell other people to use this system."

2. Respondents trusted the voting system, and this correlated strongly (Spearman's correlation coefficient $r(43) = 0.57$; two-tailed $p < 0.001$) with the voter agreeing with the system being easy to use. Just over 60% of respondents had no concerns regarding e-voting security.

3. Respondents found the verification lists easy to use. About half of the respondents responded positively to having compared the CL and PR lists together.

4. About 40% stated they were Very Likely or Likely to verify their receipt on the VEC website. In fact there were around 150 receipt lookups, about 13% of the electronic votes cast.

5. Many respondents did not understand the purpose of the verification measures. This is evident in low correlation ($r(43) = -0.14$, $p = 0.35$) between "compared CL and PR" with "I understand the printed receipt". More than half of respondents thought that the voting receipt gave away the content of their vote, which is not the case. However, for people "concerned about e-voting", comprehension of the receipt was much better: only a quarter felt the receipt leaked their vote.

6. An important question from the instrument of [14] asked if voters *still trusted the system* given the survey questions about potential threats. The voters concerns remained unchanged or even strengthened ($r(43) = 0.80$, $p < 0.001$).

7. One desired outcome of the survey was not observed: that at least some respondents would use verification measures *because* they have concerns about e-voting. That is, the survey could not detect the kind of vigilance that the verification relies on via significant negative correlations between "trust" and "use of the verification measures" despite strong negative correlation ($r(43) = -0.61; p < 0.001$) between the e-voting security question and the question about trust of the system.

Poll worker surveys

The **poll worker** surveys were conducted after the end of the election. There is some over-reporting as may be expected since the survey responses can include the same events reported separately. The summary of findings is:

1. System features for accessibility were well used. A quarter of respondents set font or contrast for voters, with forty percent setting audio mode. Twelve percent of respondents reported setting a non-English language.

2. The system did not require much intervention in the voting session, and when this occurred, the intended support tools were used. In up to 10 cases in Victoria, staff had to complete the e-vote for voters, and could see the vote being cast. This is a privacy issue that requires further consideration. A quarter of staff respondents reported using the *switch to visual* support feature to help an audio voter in-session. No respondents needed to use the *switch to English* support feature.

3. The verifiability measures were well used. A quarter of respondents saw voters perform CL-PR. Only two respondents handled voters reporting the PR did not match their vote.

4. Staff may have not fully understood verifiability. Three quarters of respondents stated they Strongly Agree or Agree to understanding verifiability and the printed lists. However, the same respondents answered differently to questions asking them about the lookup of receipts on the web and of CL audit.

5. Although more than half of respondents stated the system was Too Difficult to Operate or Not Very Reliable, two thirds stated they would be happy to support it if more voters came to use it. One third stated a negative opinion about e-voting.

6. Staff need more aides to support this system. Two thirds stated the tablets needed to offer more help. Half of respondents stated they needed more training which correlated with a quarter reporting they got questions they could not answer, that they would like to know more and that a quarter did not practice audio voting, or 20% did not use training mode at all.

Web lookups

The vVote suite of pages on vec.vic.gov.au were all visited with increasing frequency up to Election Day. Pages such as the Electronic Voting page were hit more than 20,000 times, by 18,600 unique viewers. There were 150 receipt lookups, 139 accesses to the verification data files, and 55 hits of the source code repository.

Voters accessed support documents such as locations of assistive voting centres (950), information about electronically assisted voting (554), and the Demtech assessment of vVote (35).

People accessing the vVote suite of pages came most frequently from LinkedIn (90) and Vision Australia (54) and Twitter (24), among others. Google search outside of VEC was used to access this suite 1071 times with 24 site-internal searches for 'Electronic Voting'.

Availability and time to vote

1. The Web Bulletin Board systems were up 100% with no errors. Average response (reply) time was 0.3 seconds.

2. A full analysis of the log files showed that no unexpected exceptions occurred during live voting.

3. London was offline intermittently, totalling about 14 hours of downtime over the two weeks due to networking problems. Voters affected by this voted on paper ballots.

4. London reported queuing and some network problems and Victoria served voters with a range of barriers and impairments.

In London the vast majority of voters voted without requesting accessibility or language settings. They may have made their own settings in this regard once on the EBM. Staff observed only four voters using a non-visual mode of voting and about the same number using a non-English language.

5. The average voting session time at the EBM was 172.2 seconds (about 3 minutes), with Above Line averaging 152.6 seconds, and Below Line (giving at least 5 preferences) averaging 270 seconds.

In Victoria all eligible voters were either low vision or totally blind; could not read in English; or, had a fine motor impairment or illiteracy.

6. The average voting session time was 570.4 seconds (about 9.5 minutes), with Above Line averaging 542.8 seconds and Below Line averaging 658.3 seconds.

The proportion of formal (unspoiled) electronic votes was 98.13%, with 29 informal votes in District races (2.5%), and 13 informal votes in Region races (1.15%). Paper election informality in 2014 was 5.22% district, 3.43% region. The voting system provides warnings for informal or blank votes both with audio and in-language. It is unlikely voters who cast informal votes did so unintentionally.

7 Discussion and Lessons learned

A number of serious concerns on low rates of E2EV verification among voters and some previous negative usability findings for Prêt à Voter appear to have been mitigated in this work and as such E2EV in the Victorian deployment appears likely to be a repeatable and possibly scalable result with some changes to staff and voter education.

There was an inevitable tension between the desire to allow voters to "vote and go" (i.e. to keep the voting experience as lightweight as possible, and reduce queuing) and the need to have security steps that some of the voters follow, to ensure verifiability. The voter surveys found that the voters were generally satisfied with their voting experience, so the security elements did not obstruct the voting process for them, and those that wanted to vote and go were able to do so. Voters did not resist the verifiability features as was observed (of a different system) in [14].

However, comprehension was low as was seen in [14], despite vVote being a live election and not an experiment, indicating that more work is needed to find the balance between educating voters before and during voting, and instructing them to perform verification measures in session without the risk of considerable delay in the voting ceremony. The lack of comprehension of the verification measures does not impact election integrity unless the misunderstanding means that verification audit failures are not detected.

Possibly the most serious problem in this deployment was the absence of ballot audits. The staff were trained to perform this and support it but this facility was not promoted to voters. This is one of the five or so audits and challenges provided in the data flow of vVote and ballot audit is very important for catching influence (and bugs) in the VPS device. Note that problems with ballot generation on VPS would have been caught in the self-audit done at ballot generation time and so it is reasonable to assume ballots were well formed. It is also the case that a range of failures and attacks affecting printed CLs would be picked up by the EBM *unless* the VPS and EBM collude. If this occurred votes could be "switched" so that a vote cast for Alice would become a vote for Bob. A proportion of voters (and staff or others) performing ballot audits would identify this behaviour, and so this must be done in ongoing deployments. More work is needed for future deployments to make Ballot Audit simple and quick for both staff and voters so that is it provided in accordance with the system protocol. It should be noted that even without any ballot audits having occurred, the deterrent value of ballot audits occurring *was still present* since the facility to audit was there for any and all who may have been told to do it. For example, the University of Melbourne published a plain language voter guide for vVote explaining all of the audits [15].

Almost half of the staff survey respondents (a quarter of staff) reported the system was difficult to operate or unreliable. Unfortunately there were technical problems at the start of election which affected bandwidth to VEC and there was a missing instruction in the setup manual. However, these issues were resolved quickly and the rest of the run was largely problem free. That the London site could collect more than 900 votes identified that a poll place with vVote could process good numbers of voters largely without issue.

It was a tabled risk that the Prêt à Voter voting receipt randomisation of preferences would cause voters who checked them to think their actual vote had been changed. For this reason, all surveys included questions about this. The results show there were some isolated cases of confusion (six) which were resolved satisfactorily. It is not the case that voters reported, or staff observed, voters substantially confused about the content of verification receipts.

It should not be the case that polling place staff require a deep technical understanding of vVote (or cryptography) but it is the case that staff have to answer questions or direct voters to answers about many aspects of vVote and up to 15% of poll staff reported one or more instances of questions they could not answer. Staff need to be reassured that they (and the voters) do not need this expertise in order to take part in the election. In 2014 many voters thought the voting receipt was secret. This belief does not

impose a risk to the voter or their vote but should be addressed at least so the voter can share the receipt with others who can also verify it online.

Staff-voter time is very limited and the paper voting process has enjoyed many years of optimisations and refinements, so that staff are confident in the process, and this must impact positively on voters. In contrast, if the E2EV scheme is mysterious and staff are not trained to competence and confidence then this too will be evident to voters who may refuse to use the system or refuse to fully exploit it. As with proportional vote hand counting, which is not fully understood by most Australians, it remains to be seen how deeply E2EV concepts are learned by most or whether most voters trust that others will understand them. The difference is that E2EV requires a measure of real vigilance from voters who are relied on to individually test the system for problems.

Finally, the server system was entirely housed at VEC. As reported an unrelated technical problem did indeed impact vVote at the start of the election because bandwidth was limited. To mitigate this, vVote servers should not be housed together, for both disaster recovery reasons and also for the Electoral Commission's plausible deniability in keeping hands off systems that can otherwise collude or be observed together. That is, there is a privacy risk when services are homogeneously provided and overseen by the same entity: since one entity oversees all cooperating nodes, it may be possible for them to align an voter with their vote. A future deployment should explore how heterogeneous implementations of the protocol can be served from different machines at different hosts. The design wholly anticipates this and it would bring back to e-voting the great value of mutually distrusting stakeholders having a meaningful oversight of the process: stakeholders can provide a computing node of their own making and vVote operates on the quorum of cooperating services.

8 Open Source Project

Although the system was developed for use in the State of Victoria, much of it can be customised to elections elsewhere. All the software deployed in this report, including utilities and Android operating system customisations are GPL3 at bitbucket.com/vvote. Documentation, the voter survey, and other materials from the project are also included under /doco. The design of vVote is such that it can be adapted to any kind of ballot style or process for example single choice, multiple choice, preference voting, or alternative vote. We hope the findings of this report and techniques present in the software sources lead to greater use of this approach to electronic voting.

Acknowledgements

We are grateful to our colleagues Prof. Peter Ryan and Dr. Vanessa Teague for their substantial voluntary contribution to the deployment of the system. Thanks to the Victorian Electoral Commission executive and polling staff. Thanks also to the anonymous referees for their thorough and detailed comments. The underlying research was funded by EPSRC under grant EP/G025797/1, 'Trustworthy Voting Systems', and under EP/K503939/1.

Data Access Statement: The DOI for the dataset is 10.15126/surreydata.00808345. All data generated by the University of Surrey are available without restriction. Due to confidentiality agreements some of the supporting data can only be made available with the permission of VEC.

References

[1] M. McKenna, *Building 'a closet of prayer' in the New World: the story of the Australian Ballot*, vol. 6 of *London Papers in Australian Studies*. King's College London, University of London, 2002.

[2] EAC, "Voluntary voting system guidelines." US Election Assistance Commission, 2007.

[3] R. L. Rivest, "On the notion of 'software independence' in voting systems," *Philosophical Transactions of the Royal Society A: Mathemati-*

cal, Physical and Engineering Sciences, vol. 366, no. 1881, pp. 3759–3767, 2008.

[4] C. Schürmann, D. Basin, and L. Ronquillo, "Review of the vVote system," Tech. Rep. DemTech/VEC/Report1, DemTech, March 2014.

[5] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy," in *Proc. USENIX Security*, 2010.

[6] T. Kaczmarek, J. Wittrock, R. Carback, A. Florescu, J. Rubio, N. Runyan, P. L. Vora, and F. Zagórski, "Dispute resolution in accessible voting systems: The design and use of audiotegrity," in *Proc. E-Voting and Identify*, LNCS 7985, pp. 127–141, 2013.

[7] F. Zagórski, R. Carback, D. Chaum, J. Clark, A. Essex, and P. L. Vora, "Remotegrity: Design and use of an end-to-end verifiable remote voting system," in *Proc. Applied Cryptography and Network Security*, pp. 441–457, 2013.

[8] J. Benaloh, R. L. Rivest, P. Y. A. Ryan, P. B. Stark, V. Teague, and P. L. Vora, "End-to-end verifiability," *CoRR*, vol. abs/1504.03778, 2015.

[9] F. Hao and P. Y. A. Ryan, eds., *Real-World Electronic Voting: Design, Analysis and Deployment*. Auerbach Publications (to appear), 2015.

[10] D. Chaum, P. Y. A. Ryan, and S. A. Schneider, "A practical voter-verifiable election scheme," in *Proc. European Symposium on Research in Computer Security*, LNCS 3679, pp. 118–139, 2005.

[11] C. Z. Acemyan, P. T. Kortum, M. D. Byrne, and D. S. Wallach, "Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II," in *Proc. Electronic Voting Technology/Workshop on Trustworthy Elections*, 2014.

[12] S. Schneider, M. Llewellyn, C. Culnane, J. Heather, S. Srinivasan, and Z. Xia, "Focus group views on Prêt à Voter 1.0," in *Proc. Requirements Engineering for Electronic Voting Systems*, pp. 56–65, IEEE, 2011.

[13] C. Culnane, P. Y. A. Ryan, S. Schneider, and V. Teague, "vVote: a verifiable voting system," *ACM Transactions on Information and System Security*, vol. 18, no. 3, 2015.

[14] F. Karayumak, M. Kauer, M. M. Olembo, T. Volk, and M. Volkamer, "User study of the improved Helios voting system interfaces," in *Proc. Socio-Technical Aspects in Security and Trust*, pp. 37–44, 2011.

[15] V. Teague, "Click here for democracy: the e-vote explained." http://electionwatch.edu.au/victoria-2014/click-here-democracy-e-vote-explained, 2014.

Craig Burton was Special Projects Manager at the Victorian Electoral Commission and overall lead for the vVote project. Contact him at c.burton@coasca.com

Chris Culnane was System Architect at Surrey on the vVote project. Contact him at acad@chrisculnane.com

Steve Schneider is Professor in Security and Director of the Surrey Centre for Cyber Security at the University of Surrey. Contact him at s.schneider@surrey.ac.uk.