vVote: Verifiable Electronic Voting in Practice

Craig Burton | Victorian Electoral Commission
Chris Culnane and Steve Schneider | University of Surrey

In Victoria, Australia, the vVote verifiable voting system allowed blind voters and voters in remote locations to cast fully secret ballots in a verifiable way. The new verifiability checks didn't impede function or satisfaction in the voting experience.

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

In this article, we describe the experience of deploying the vVote verifiable voting system in the November 2014 state election in Victoria, Australia; report the voters' and poll workers' experience with the system; and discuss its end-to-end verifiability (E2EV). (For more information on verifiable electronic voting, see the sidebar.)

History of Voting in Victoria

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 with government-printed ballots, logistic checks and balances, and private booths.[1] More recently, the Victorian Electoral Commission (VEC) was an early adopter of electronic voting and fielded systems in 2006 and 2010. The 2002 Electoral Act's amendments for electronic voting in Victoria intended better accessibility for blind, partially sighted, and motor-impaired voters via customized computer voting interfaces; for voters speaking languages other than English; and for voters out of state and overseas, enabling more rapid returns of those votes into the tallying process.

Australia has no e-voting standards or guidelines (except the voluntary Telephone Voting Standards), so the VEC was guided by the US Voluntary Voting System Guidelines, as these were seen to be the most recent and progressive guidelines to consider networked IT security threats.[2] In addition, software independence is a critical basis for trustworthy voting systems: "an undetected change or error in the software cannot cause an undetectable change or error in the election outcome."[3] 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]

Victoria's election system poses particular challenges for any verifiable solution because of the complexity of its ballots. In state elections, voters vote in two races. For the Legislative Assembly, voters rank all candidates

1540-7993/16/$33.00 © 2016 IEEE

Related Work in Verifiable Electronic Voting

Aside from vVote, the only statutory end-to-end verifiable elections to date have taken place in Takoma Park, Maryland, where the Scantegrity system was successfully used in 2009 and 2011 in the municipal election for mayor and city council members.[1] Scantegrity has been adapted and trialed for remote voting (“Remotegrity”) as well as voting for blind voters (“Audiotegrity”).[2,3] This groundbreaking work demonstrated the feasibility of running an election in a verifiable way, including with people who have physical obstacles to voting. However, the Scantegrity system is impractical for a preferential ballot of up to 40 candidates. Preferential ordering of only 5 of the 40 candidates might already require 200 check boxes (combining candidate and preference); ordering all 40 would require many more.

There is a rich body of work covering remote voting, direct-recording electronic machines, and many other systems, which we can’t summarize here. We’re specifically pursuing end-to-end verifiability (E2EV) at scale, and as such, this is the first work of its kind. We direct the reader elsewhere for an introduction to verifiability in electronic voting systems and to coverage of related systems.[4,5]

E2EV—an approach to computer security designed specifically for elections—provides highly reliable detection of loss, damage, or fraud that affects votes. It’s not a method of defense, but it does provide an important new deterrent because attackers must consider the likelihood of detection. Many current security systems can report only detected attacks. E2EV detects, with high probability, attempts to change the election outcome, whether or not the voting system software performs as expected—this is software independence. vVote was created to safely collect votes in a verifiable manner, replacing the previous third-party system that was not end-to-end verifiable.

References

1. R. Carback et al., “Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy,” *Proc. 19th USENIX Conf. Security*, 2010, pp. 291–306.
2. F. Zagórski et al., “Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System,” *Proc. 11th. Int’l Conf. Applied Cryptography and Network Security*, 2013, pp. 441–457.
3. T. Kaczmarek et al., “Dispute Resolution in Accessible Voting Systems: The Design and Use of Audiotegrity,” *Proc. 4th Int’l Conf. E-Voting and Identify*, LNCS 7985, 2013, pp. 127–141.
4. J. Benaloh et al., “End-to-End Verifiability,” *Computer Research Repository*, abs/1504.03778, 2015.
5. *Real-World Electronic Voting: Design, Analysis and Deployment*, F. Hao and P.Y.A. Ryan, eds., to be published by Auerbach, Oct. 2016.

in preferential order, usually up to 10 candidates. For the Legislative Council, voters either select one party or group (“above line”) or rank the individual candidates—typically up to 40—in their preferred order (“below line”).

There are eight regions comprising 88 districts, so there are 96 races in total. Nominations for candidates were open until noon on Friday, 14 November 2014, and the electronic system needed to be ready to take votes beginning Monday, 17 November. A two-week period of early voting, for which the electronic system was deployed, ran until the official election day, Saturday, 29 November. Electronic voting was available only during early voting and voters were allowed to use any polling station to cast a ballot in their home races. Thus, all polling stations needed to offer ballot forms for all 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 (www.abs.gov.au/ausstats) indicates that as many as 186,000 Victorian travelers, 100,000 adults not proficient in English, and 118,000 adults with low vision or blindness were eligible to vote using the electronic system. A total of 1,121 votes were collected. This was more votes than were collected by the 2010 electronic system, even though the system was deployed at fewer locations (25 instead of 101).

System Description

The starting point for vVote design was the Prêt à Voter split ballot (see Figure 1).[5] Because the paper-based Prêt à Voter method has differing usability assessment results in its paper form, considerable work went into its electronic form.[6,7] It was mandated that accessibility must extend to polling-place verification. (The completed technical design of the system as deployed is described elsewhere, where comparisons to other electronic voting schemes are also discussed.[8])

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 voters are marked off the electoral roll, they’re given a printed candidate list (CL) with the names in a random order. Voters can request that their CL be

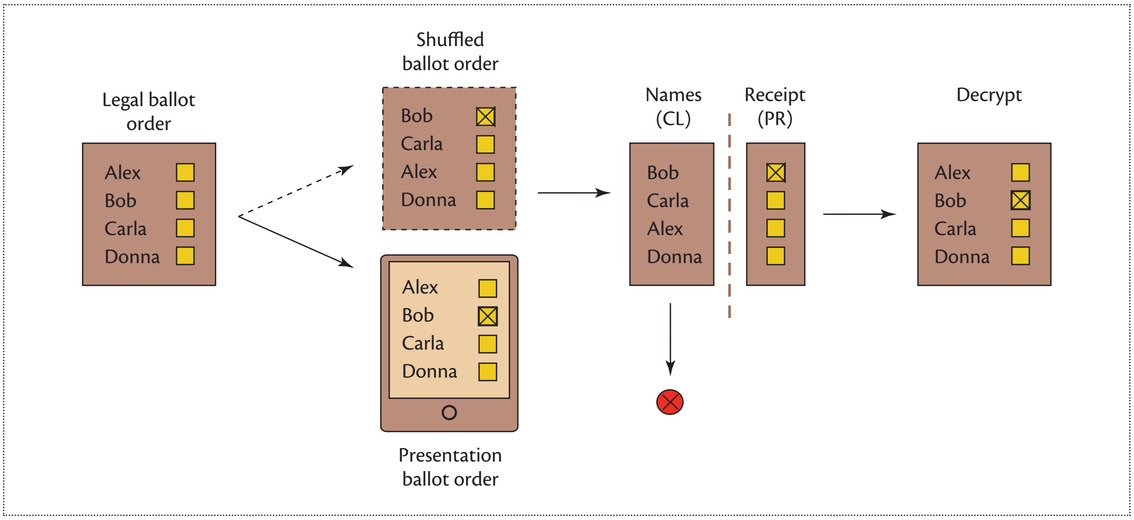


Figure 1. Prêt à Voter with an electronic ballot marker (EBM). The legal ballot order (left) is shuffled to create candidate lists (CLs). The presentation order in paper Prêt à Voter is shuffled (top ballots). The vVote ballot (shown on an EBM) is the legal order. The tablet reads the CL and, upon receiving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

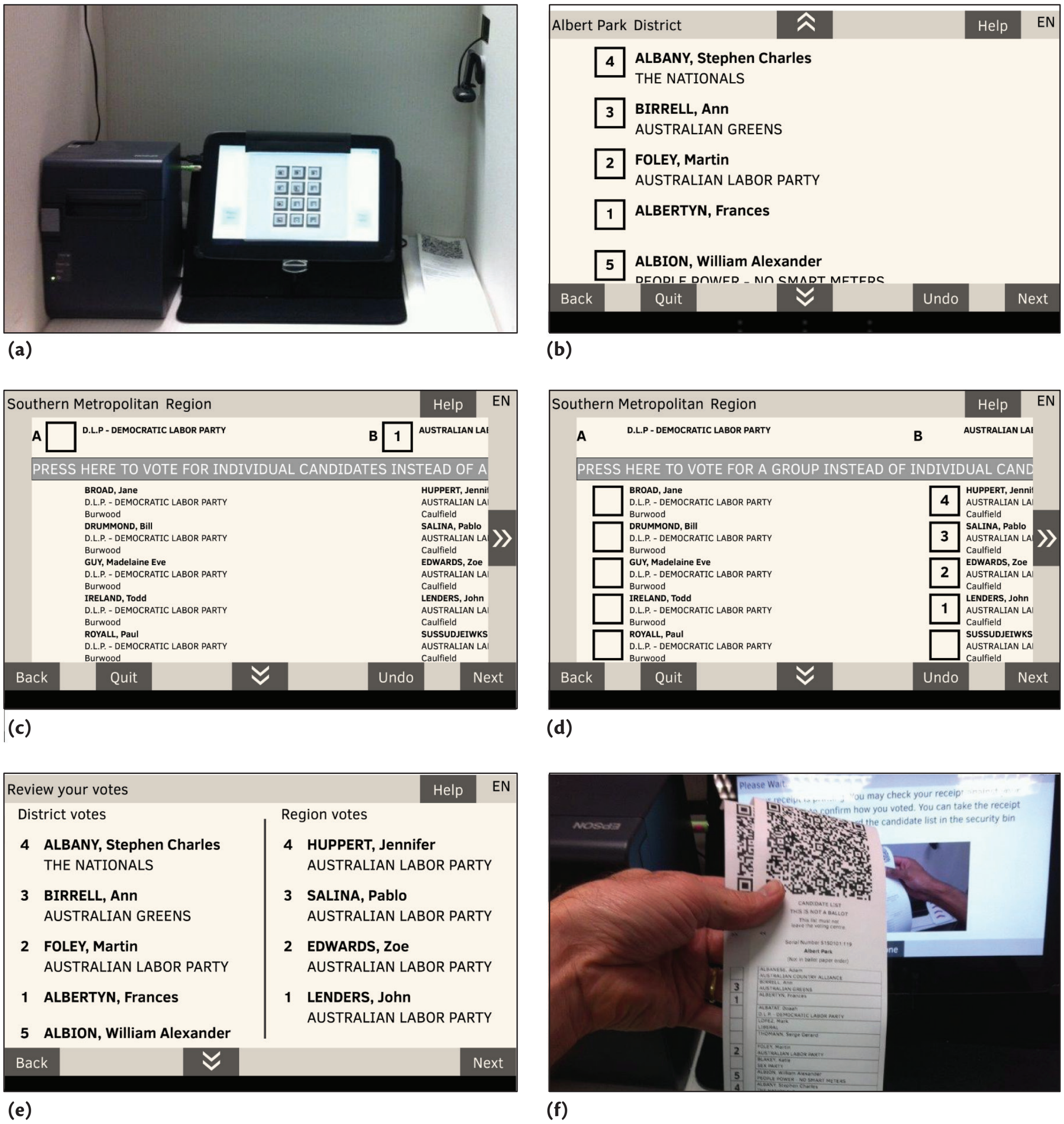
audited to check that the printed order matches the encrypted order to which the system has already committed. An audited CL can't then be used to vote, and all such audit results are made public automatically. Following an audit, voters are issued a new CL. In the 2014 deployment, voters weren't alerted to this possibility because 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, and that it could cause delays and queuing. For future deployments, some education presented in advance would raise awareness of this step.

When voters use a CL to vote, an external camera attached to the tablet reads the list. The booth setup for blind voters is illustrated in Figure 2a, 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 the QR code for the CL launches the vote capture application, which allows voters to enter their vote. The EBM interface for sighted voters is illustrated in Figures 2b–e. After a vote is submitted, a preferences receipt (PR) is printed separately. Voters verify that the preferences match the correct candidate names by comparing the lists side by side, as in Figure 2f, or via audio means. This check ensures that the receipt captures the vote as cast. Once this is done, the CL is destroyed to keep the vote secret. Voters retain their PR. The fact that the candidate names were in a shuffled order ensures that the PR doesn't expose voter preferences and thus provides ballot secrecy.

The system allows staff to "quarantine" or cancel a vote if the PR is not provided for any reason, if a voter considers the PR to be incorrect, or if a voter reports serious usability issues. Voters 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 can't occur silently. Bulk quarantine—a mechanism whereby the electoral commission can exclude all votes from one device from being decrypted—occurs outside the protocol and is considered a manual intervention. In the deployment, there were six 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).

Voters later look up their PR on the WBB and verify that it's been included properly; they can raise a challenge if it has not. At any time, voters (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 to check the PR signature against the public key for the election to confirm that the central recording system signed the return. This functionality was available during deployment, though not promoted.

It's important to add that all aspects of the voting process, as well as the verification measures intended for voters, are also made accessible. A ballot audit can be taken to an EBM, and the device will read the contents out loud. Both the CL and PR can be read out separately on any EBM or, if provided together (to give the shuffled order of candidate names if required),



(b)

Albert Park District — Help — EN

4 **ALBANY, Stephen Charles**
THE NATIONALS

3 **BIRRELL, Ann**
AUSTRALIAN GREENS

2 **FOLEY, Martin**
AUSTRALIAN LABOR PARTY

1 **ALBERTYN, Frances**

5 **ALBION, William Alexander**
PEOPLE POWER - NO SMART METERS

Back — Quit — Undo — Next

(c)

Southern Metropolitan Region — Help — EN

A □ D.L.P - DEMOCRATIC LABOR PARTY — B 1 AUSTRALIAN LA

PRESS HERE TO VOTE FOR INDIVIDUAL CANDIDATES INSTEAD OF A

BROAD, Jane D.L.P. - DEMOCRATIC LABOR PARTY Burwood	**HUPPERT, Jennif** AUSTRALIAN LA Caulfield
DRUMMOND, Bill D.L.P. - DEMOCRATIC LABOR PARTY Burwood	**SALINA, Pablo** AUSTRALIAN LA Caulfield
GUY, Madelaine Eve D.L.P. - DEMOCRATIC LABOR PARTY Burwood	**EDWARDS, Zoe** AUSTRALIAN LA Caulfield
IRELAND, Todd D.L.P. - DEMOCRATIC LABOR PARTY Burwood	**LENDERS, John** AUSTRALIAN LA Caulfield
ROYALL, Paul D.L.P. - DEMOCRATIC LABOR PARTY Burwood	**SUSSUDJEIWKS** AUSTRALIAN LA Caulfield

Back — Quit — Undo — Next

(d)

Southern Metropolitan Region — Help — EN

A D.L.P - DEMOCRATIC LABOR PARTY — B AUSTRALIAN LA

PRESS HERE TO VOTE FOR A GROUP INSTEAD OF INDIVIDUAL CAND

□	**BROAD, Jane** D.L.P. - DEMOCRATIC LABOR PARTY Burwood	4	**HUPPERT, Jennif** AUSTRALIAN LA Caulfield
□	**DRUMMOND, Bill** D.L.P. - DEMOCRATIC LABOR PARTY Burwood	3	**SALINA, Pablo** AUSTRALIAN LA Caulfield
□	**GUY, Madelaine Eve** D.L.P. - DEMOCRATIC LABOR PARTY Burwood	2	**EDWARDS, Zoe** AUSTRALIAN LA Caulfield
□	**IRELAND, Todd** D.L.P. - DEMOCRATIC LABOR PARTY Burwood	1	**LENDERS, John** AUSTRALIAN LA Caulfield
□	**ROYALL, Paul** D.L.P. - DEMOCRATIC LABOR PARTY Burwood	□	**SUSSUDJEIWKS** AUSTRALIAN LA Caulfield

Back — Quit — Undo — Next

(e)

Review your votes — Help — EN

District votes		Region votes	
4	**ALBANY, Stephen Charles** THE NATIONALS	4	**HUPPERT, Jennifer** AUSTRALIAN LABOR PARTY
3	**BIRRELL, Ann** AUSTRALIAN GREENS	3	**SALINA, Pablo** AUSTRALIAN LABOR PARTY
2	**FOLEY, Martin** AUSTRALIAN LABOR PARTY	2	**EDWARDS, Zoe** AUSTRALIAN LABOR PARTY
1	**ALBERTYN, Frances**	1	**LENDERS, John** AUSTRALIAN LABOR PARTY
5	**ALBION, William Alexander**		

Back — Next

(f)
Please Wait
You may check your receipt
confirm how you voted. You can take the receipt
the candidate list in the security bin
EPSON
CANDIDATE LIST
THIS IS NOT A BALLOT
Albert Park

Figure 2. Physical and graphic interfaces. (a) A voting booth for use by blind voters. A tactile latex “telephone keypad” overlay sits on the touchscreen, and headphones provide audio instructions. (b) District ballot visual interface showing preferences assigned. Voters must number all candidates and can scroll the ballot with double arrows. (c) Region ballot showing required above-line preference assigned. Voters must choose one party or group. (d) Region ballot showing below-line preferences assigned. Voters must number five or more candidates. (e) Summary of preferences for both races in legal ballot order. (f) Visual matching of the candidate list and preference receipt.

the assembled preference-order vote can be read back to voters.

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’s publicly verifiable that the correct tally is returned and counted as recorded because the mixing and decrypting of the encrypted votes generates cryptographic proofs that can be checked independently. This provides a chain of links all the way from the initial creation of blank ballots to vote casting to tallying.

In this election, the electronic votes needed to be combined with paper votes, so the electronic votes were printed off to be included in 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 to spot audits. In this case, we have verifiability for the decrypted votes: any cast vote made it into the paper count, which was then counted in the usual way.

Staff Training and Voter Support

E2EV concepts are very new, and some are inconsistent with paper election procedures. For example, the presence of E2EV ballot audits as an option voters can pursue isn't 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 doesn't allow for removal of a vote from the ballot box.

> **"Voters verify that the preferences match the correct candidate names by comparing the lists side by side, or via audio means, to ensure the receipt captures the vote as cast."**

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 before the election. Previous systems created ballots as needed, potentially at an uncontrollable quantity. Despite similarities, some new concepts, such as the random permutation of candidates, also made training more difficult. Trainees and VEC elections staff weren't certain how many questions voters would ask and how to answer them quickly without obscuring transparency aspects of the system design. It's likely that longer-term E2EV will settle in the public consciousness the same way that single transferrable vote (STV) counting is accepted but not fully understood by most Australians. Low STV comprehension might be lamentable, but in fact, those who don't understand it trust that it's performed and enforced correctly. We hope this situation evolves for E2EV as well.

During development, iterations of the system were tested under controlled conditions, and the same verbal instructions were given to cohorts of target users who were provided to VEC via disability organizations and community groups. In total, more than 150 people were videotaped using the system at least once, and the system was modified to log interface events (although this was removed before the live election). The cohorts included functionally blind users; 10 users with a range of low-vision conditions, including retinopathy and tunnel vision; eight Arabic and 10 Mandarin speakers; more than 100 nondisabled English speakers (including VEC sessional and permanent staff); and five subjects who were profoundly physically disabled with normal cognitive function and vision.

We learned a lot from this process and tested the many system changes. 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 the many trials that shaped the current system. Perhaps the most interesting observation was that the system was found to be unusable by some non-English speakers because candidate and party names were all voiced and displayed in English. It was commonly assumed that even non-English speakers could pattern match popular party names if they weren't in first languages, or that they could transpose advised voting preferences from the party literature (called the How to Vote Card—HTVC) given to voters upon arrival at all polling places. Under testing for the first time with non-bilinguals, Arabic-speaking subjects couldn't, for example, find and vote for the Green Party, even with an Arabic-language HTVC. In this case, a change request was raised, and the system was modified so that touching any party name (still in English) 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 that had previously assessed electronic voting interfaces in Australia. Inclusive UX didn't have a remit to perform its own testing due to time constraints but was given a fully working system and asked 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 (such as fully stating where the audio cursor is on the CL ballot candidate grid).

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 centers around Victoria, including the six "accessibility supercenters" set up by VEC to provide all forms of accessible voting. One was also deployed in the Australia Centre, London, UK, to gain experience using the remote voting solution with voters who had no barriers to voting. The London center was run in the same manner as the Victorian centers.

The total number of votes received over the two weeks was 1,121, of which 973 were from London and the remaining 148 from the 24 centers in the State of Victoria.

The system was developed for much higher demands to scale up for future elections: it handled 1 million votes in testing and, under stress, was able to respond to individual voters within 10 seconds and to accept 800 votes in a 10-second period.

Outcomes

Various instruments were used to obtain feedback on this project. Participant numbers were small, so the results are indicative and suggest issues for deeper investigation. A University of Surrey survey that intercepted 45 voters leaving the Australia Centre in London after casting 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 using questions taken from Fatih Karayumak and his colleagues' survey instrument.[9] VEC also ran a separate opt-in survey for London voters who volunteered their email addresses (60 responses) as well as for Victorian voters (fewer than 10 responses).

We used server logs to analyze time to vote. Google Analytics collected information for public-facing information and lookup services (not the voting system). It should also be noted that the voting protocol doesn't capture voting interface navigation actions (as it allows no metadata) and that the EBM is stateless. These privacy controls prevented capture of live usability data, such as navigating, changing languages, or undoing vote choices.

Two technical problems likely affected survey results. When the system went from training mode to live voting mode, there was a missing instruction step in the setup manual for poll workers. The absence of this setup step caused the receipt printer to not 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 during the first day of voting. The 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 29-Mbyte configuration file. Three sites weren't online at the start of voting. This problem was largely resolved by the second day of voting, but London had to revert to paper ballots for two full days in total. Setup problems in Victoria might have impacted the few voters who attended several sites, causing a disproportionate problem.

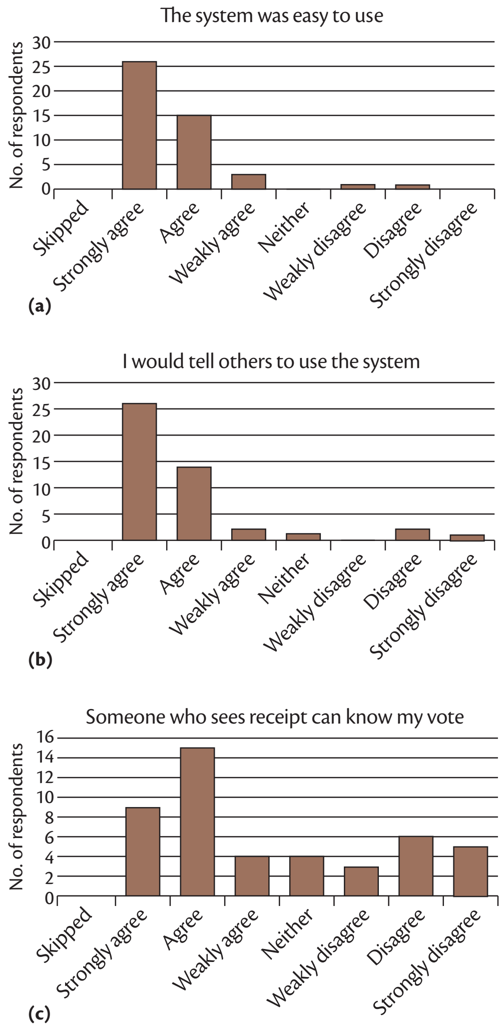


Figure 3. Three questionnaire responses from London's remote voting site: (a) and (b) show that respondents found the system easy to use and would tell others to use it, but (c) shows that, in some cases, they didn't understand the verification measure, as demonstrated by their agreement with the incorrect statement that the receipt reveals their vote.

Voters were generally satisfied with system usability, but there was a wide variation in their understanding of the security assurances. 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). Questionnaire 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. This reflected the finding reported by Karayumak and his colleagues that there was no resistance to new steps.[9] Data collected in Victoria was for very low numbers of voters, so we focused on the London results for our general findings. More work is certainly needed to accurately measure E2EV in a live polling place for both staff and voters, including expectations, error coping, and comprehension.

Respondents found the system easy to use, as Figure 3 illustrates. Seventy-five percent or more of respondents agreed or strongly agreed with all positive aspects of usability. Seventy-five percent stated they preferred the system to paper voting; this is also evident from comments and in the time taken to vote. Sixty percent of respondents voted in under four minutes and 96 percent voted in under 10. This measurement included the time to vote on the system (not the time to get a PR or wait in queues). None stated the process took "too long." In addition, 87 percent stated they agree or strongly agree with the statement "I would tell other people to use this system."

Respondents trusted the voting system, and this correlated strongly (Spearman's correlation coefficient $r(43) = 0.57$, two-tailed $p < 0.001$) with the voters expressing that the system was easy to use. Just over 60 percent of respondents had no concerns regarding e-voting security. Respondents found the verification lists easy to use. Approximately half of the respondents responded positively to having compared the CL and PR lists together. About 40 percent of respondents stated they were likely or very likely to verify their receipt on the VEC website. In fact, there were approximately 150 receipt lookups, about 13 percent of the electronic votes cast.

Many respondents didn't understand the purpose of the verification measures. This is evident in low correlation ($r(43) = -0.14$, $p = 0.35$) between responses to two survey questions: "compared CL and PR" and "I understand the printed receipt." More than half the respondents thought that the voting receipt gave away the content of their vote, which isn't the case. However, for people who indicated that they were "concerned about e-voting," comprehension of the receipt was much better: only a quarter thought that the receipt leaked their vote.

An important question from Karayumak and his colleagues' instrument asked if voters still trusted the system, given the survey questions about potential threats.[9] The voters' concerns remained unchanged or even strengthened ($r(43) = 0.80$, $p < 0.001$).

One desired outcome of the survey wasn't observed: that at least some respondents would use verification measures because they have concerns about e-voting. That is, the survey couldn't 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 overreporting, as the survey responses can include the same events reported separately.

Accessibility features were used well. A quarter of respondents set font or contrast for voters, with 40 percent setting audio mode. Twelve percent of respondents reported setting a non-English language.

The system didn't 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 switching to the visual support feature to help an audio voter in session. No respondents needed to switch to English support.

The verifiability measures were used well. A quarter of respondents saw voters perform a CL-PR check. Only two respondents had voters report that the PR didn't match their vote.

Staff might not have fully understood verifiability. Three-quarters of respondents stated they strongly agree or agree that they understood verifiability and the printed lists. However, the same respondents answered differently to questions asking them about the lookup of receipts on the Web and CL audit.

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.

We also learned that staff need more aides to support this system. Two-thirds stated that the tablets needed to offer more help. Half of the respondents stated they needed more training, which correlated with a quarter reporting that they were asked questions they couldn't answer, and that they would like to know more. A quarter didn't practice audio voting, and 20 percent didn't use the training mode at all.

Web Lookups

The vVote suite of pages on www.vec.vic.gov.au were all visited with increasing frequency up to election day. Pages such as the electronic voting page had more than 20,000 hits 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 centers (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), Vision Australia (54), and Twitter (24). Google searches outside VEC were used to access this suite 1,071 times, with 24 internal site searches for "electronic voting."

Availability and Time to Vote

The WBB systems were up 100 percent of the time, with no errors. The average response or reply time was 0.3 seconds. A full analysis of the log files showed that no unexpected exceptions occurred during live voting.

The London center was offline intermittently—approximately 14 hours of downtime over the two weeks—due to networking problems. Voters affected by this voted using paper ballots. The London center also reported queuing and some network problems. In London, the vast majority of voters voted without requesting accessibility or language settings. They might have made their own settings in this regard once on the EBM. Staff observed only four voters using a nonvisual mode of voting and about the same number using a non-English language. In Victoria, all eligible voters either had low vision or were totally blind, couldn't read in English, had a fine motor impairment, or were illiterate.

> **"The surveys found that voters were generally satisfied with their voting experiences, so the security elements didn't obstruct their voting process."**

In London, the average voting session time at the EBM was 172.2 seconds (approximately three minutes), with above line averaging 152.6 seconds, and below line (giving at least five preferences) averaging 270 seconds. In Victoria, the average voting session time was 570.4 seconds (approximately 9.5 minutes), with above line averaging 542.8 seconds and below line averaging 658.3 seconds.

The proportion of formal (correctly formed and corresponding to a valid vote) electronic votes was 98.13 percent, with 29 informal votes in district races (2.5 percent) and 13 informal votes in region races (1.15 percent). Paper election informality in 2014 was 5.22 percent for district and 3.43 percent for region. The voting system provides warnings for informal or blank votes, both with audio and in-language systems. It's unlikely that voters who cast informal votes did so unintentionally.

Discussion and Lessons Learned

Several serious concerns on low E2EV verification rates among voters and some previous negative usability findings for Prêt à Voter appear to have been mitigated in this work; 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" (that is, to keep the voting experience as lightweight as possible and reduce queuing) and the need to have security steps to ensure verifiability. The surveys found that voters were generally satisfied with their voting experience, so the security elements didn't obstruct their voting process, and those who wanted to vote and go were able to do so. Voters didn't resist the verifiability features (as was also observed in a different system[9]).

However, comprehension was low (as was also seen in the other system[9]), 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 process. The lack of comprehension of the verification measures doesn't impact election integrity unless the misunderstanding means that verification audit failures aren't detected.

Possibly the most serious problem in this deployment was the absence of ballot audits. The staff were trained to perform and support audits, but this facility wasn't promoted to voters. Ballot audit is one of the approximately five audits and challenges the vVote dataflow provides and is very important for catching influence (and bugs) in the VPS device. Note that problems with ballot generation on VPS would've been caught in the self-audit done at ballot-generation time, so it's reasonable to assume that ballots were formed correctly.

In addition, EBM would detect a range of failures and attacks affecting printed CLs unless the VPS and EBM colluded. If this occurred, votes could be "switched" so that a vote cast for Alice could become a vote for Bob. A proportion of voters (and staff or others) performing ballot audits would identify this behavior; therefore, this must be done in ongoing deployments. More work is needed for future deployments to make ballot audits simple and quick for both staff and voters so that they're provided in accordance with the system protocol.

Note that even without any ballot audits, the deterrent value of ballot audits occurring was still present because the facility to audit was there for anyone who wanted to do so. For example, the University of

Melbourne published a plain-language voter guide for vVote explaining all the audits.[10]

Almost half of the staff survey respondents (a quarter of the total staff) reported that the system was difficult to operate or unreliable. Unfortunately, there were technical problems at the start of the election that affected bandwidth to VEC, and there was also a missing instruction in the setup manual. However, these issues were resolved quickly, and the rest of the run was largely problem free. The London site collected more than 900 votes, indicating that a poll place with vVote can process high volumes of votes largely without issue.

It was a tabled risk that the Prêt à Voter voting receipt randomization 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 six isolated cases of confusion, which were resolved satisfactorily. Voters didn't report, nor did staff observe, substantial confusion about the content of verification receipts.

Polling place staff shouldn't require a deep technical understanding of vVote (or cryptography), but staff must answer questions or direct voters to answers about many aspects of vVote. Up to 15 percent of poll staff reported one or more instances of questions they couldn't answer. Staff need to be reassured that they and the voters don't need this expertise to take part in the election. In 2014, many voters thought the voting receipt should be kept secret. This belief doesn't pose a risk to voters or their vote but should be addressed, at least so voters 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 optimizations and refinements, so staff are confident in that process, which positively impacts voters. In contrast, if the E2EV scheme is mysterious and staff aren't trained to competence and confidence, then this too will be evident to voters who might refuse to use or fully exploit the system. As with proportional vote hand counting, which isn't 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 housed entirely 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 shouldn't 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's a privacy risk when services are homogeneously provided and overseen by the same entity: because one entity oversees all cooperating nodes, it might be possible for it to link voters with their votes. 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 would provide a computing node of their own making, and vVote would operate on the quorum of cooperating services.

Although the system was developed for use in the State of Victoria, much of it can be customized to elections elsewhere. All the software deployed in this report, including utilities and Android OS customizations are GPL3 at www.bitbucket.com/vvote. Documentation, the voter survey, and other materials from the project are also included at www.bitbucket.com/vvote/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, or alternative voting. We hope the findings of this report and techniques present in the open source software lead to greater use of this approach to electronic voting. ■

Acknowledgments

We are grateful to our colleagues Peter Ryan and Vanessa Teague for their substantial voluntary contributions to the deployment of the system. We thank the Victorian Electoral Commission executive and polling staff. We also thank 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 is available without restriction. Due to confidentiality agreements, some of the supporting data can be made available only with the permission of Victorian Electoral Commission.

References

1. M. McKenna, *Building 'A Closet of Prayer' in the New World: The Story of the Australian Ballot*, vol. 6, London Papers in Australian Studies, King's College London, Univ. London, 2002.
2. "Voluntary Voting System Guidelines," US Election Assistance Commission, 2007; www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.
3. R.L. Rivest, "On the Notion of 'Software Independence' in Voting Systems," *Philosophical Trans. Royal Society A: Mathematical, Physical and Eng. Sciences*, vol. 366, no. 1881, 2008, pp. 3759–3767.
4. C. Schürmann, D. Basin, and L. Ronquillo, *Review of*

the vVote System, tech. report DemTech/VEC/Report1, DemTech, 2014.

5. D. Chaum, P.Y.A. Ryan, and S.A. Schneider, "A Practical Voter-Verifiable Election Scheme," *Proc. 10th European Conf. Research in Computer Security* (ESORICS 05), LNCS 3679, 2005, pp. 118–139.
6. C.Z. Acemyan et al., "Usability of Voter Verifiable, End-to-End Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II," *Proc. Electronic Voting Technology/Workshop Trustworthy Elections* (EVT/VOTE 14), 2014; www.usenix.org/conference/evtwote14/workshop-program/presentation/acemyan.
7. S. Schneider et al., "Focus Group Views on Prêt à Voter 1.0," *Proc. IEEE Int'l Workshop Requirements Eng. for Electronic Voting Systems* (REVOTE 11), 2011, pp. 56–65.
8. C. Culnane et al., "vVote: A Verifiable Voting System," *ACM Trans. Information and System Security*, vol. 18, no. 1, 2015; http://dx.doi.org/10.1145/2746338.
9. F. Karayumak et al., "User Study of the Improved Helios Voting System Interfaces," *Proc. 1st Workshop Socio-technical Aspects in Security and Trust* (STAST 11), 2011, pp. 37–44.
10. V. Teague, "Click Here for Democracy: The E-vote Explained," Election Watch, 2014; http://past.electionwatch.edu.au/victoria-2014/click-here-democracy-e-vote-explained.

Craig Burton was special projects manager at the Victorian Electoral Commission and overall lead for the vVote project at the time of writing. He's currently a director at Coasca. His research interests include information security, restorable elections, and human computing. Burton received a BS in computer science from the University of Melbourne. Contact him at c.burton@coasca.com.

Chris Culnane was the system architect at the University of Surrey on the vVote project. His research interests include secure systems design and implementation, with particular emphasis on voting systems. Culnane received a PhD in computer science from the University of Surrey. Contact him at acad@chrisculnane.com.

Steve Schneider is a professor in security and director of the Surrey Centre for Cyber Security at the University of Surrey. His research interests include secure electronic voting, security protocols, and verification methods for trust and privacy. Schneider received a PhD in computer science from Oxford University. Contact him at s.schneider@surrey.ac.uk.