Submission to the iVote 2019 Inquiry

Dr Roland Wen Professor Richard Buckland

Security Engineering and Cyber Governance
School of Computer Science and Engineering
The University of New South Wales

Executive Summary

This report addresses the iVote voting systems which have been developed by the NSW Electoral Commission and external vendors. The deployment of the original iVote system has been largely positive and it is commendable that the NSWEC has been able to do so much with the budget available. However this report outlines two serious security concerns:

1. that the existing system is not safe for large-scale voting where errors or security flaws could affect the outcome of an election; and

2. that a new version of the system being considered does not have sufficient time to be safely designed, implemented, deployed and tested before the 2019 State Election.

This report covers two different electronic voting systems, each commonly known as "iVote":

1. **"the existing iVote"** The existing Internet voting system which has had two versions and has been used in the 2011 and 2015 NSW elections and also the WA 2017 election. This system works well at small scale as intended but was not designed to be used at a large scale where a security vulnerability or system failure could affect who gets elected.

2. **"the new system"** To address the increased security and reliability requirements of large-scale electronic voting a new voting system is currently being developed intended for large-scale voting in 2019 and onwards. It will involve new software and a new cryptographic design and security features. The "new system" has gone to tender but its design is not yet determined.
   Our professional opinion, based on extensive study of the major electronic voting systems worldwide and an expert understanding of software and security engineering failures, is that there is insufficient time remaining to securely design, build and properly test any new system before the 2019 election. Attempting to rush a system into place by that time will pose serious risks of a catastrophic incident or election security vulnerability. Furthermore such a process will be inefficient as it will not produce software of sufficient quality to be reused in future elections.

We recommend that the existing iVote system be used at the 2019 NSW State Election on a small scale for voters with disabilities and voters living in remote regions. By small scale we mean not for so many voters that an error or attack could be reasonably expected to change the election outcome. This would likely be in the order of 100 000 votes or less.

We recommend that a new iVote system be developed for large-scale use at the subsequent 2023 State Election, and that the new system be carefully trialled at a number of local government elections and by-elections *before* being used for a full state election.

We make further recommendations about the need to design, build and scrutinise the new system at a "failure-critical" level of quality, not at "commercial" level, as it is critical national infrastructure.

We also note the benefits of collaboration between state electoral commissions in developing secure electronic voting systems so that costs can be shared and resources aggregated. We note the desirability to avoid a pattern of duplicating systems across multiple jurisdictions, of resource constraints and tight deadlines leading to lower security, and of lower quality single-use systems needing to be thrown away or substantially rebuilt each electoral cycle.

1 Introduction

The existing iVote system was designed for small-scale voting and has been used successfully in a number of elections. This has been a significant achievement given the limited budget, resources and time available to develop and operate the system. The system has provided benefits to groups of voters not served well by in polling-place voting, such as voters requiring assistance. Such groups can also be accommodated by other methods such as telephone or postal voting but there is anecdotal evidence that many such voters strongly prefer electronic voting. Furthermore there are considerable problems with slow postal delivery times potentially disenfranchising certain voters living in remote locations. Such voters have also benefited from using the system.

The existing iVote system was never designed for large-scale voting, and it followed a lower cost security design, development and assurance process for small-scale voting. However for large-scale voting where failures and security breaches could change election outcomes, the existing iVote system falls below the standard of Internet voting systems used in public elections overseas. The existing iVote system is not fit for purpose for large-scale elections. It experienced multiple live failures and vulnerabilities in 2011 and 2015. Example technical details and evidence of shortcomings are given in Section 3 below — in summary the system has critical vulnerabilities and weaknesses in its security, quality, transparency and scrutiny.

There is manifestly insufficient time remaining to design, build and test a new Internet voting system before the 2019 State Election. Australian and international experience in designing and developing electronic election systems in short time frames is that security design and testing are dangerously compromised in order to meet the immovable election deadline. We are strongly supportive of NSW and the nation building and controlling its own election systems but note that this should be treated as failure-critical national infrastructure which requires careful and appropriate design, testing and scrutiny, not approached as commercial-grade "best-effort" software as is currently intended for the new iVote.

The design and engineering of an electronic election system should be treated as requiring the same level of quality as a critical military system, not as a commercial system. We note in passing the almost daily news of commercial systems of even well-resourced multinationals being compromised or failing. It is essential that failure-critical systems such as election systems undergo extensive assurance activities and are first deployed using rigorous pilot programs that scale up gradually. For example a pilot program would start with small-scale trials at less critical election events such as individual by-elections and targeted local government elections. If successful these would be followed by a small-scale trial at a full state election and then further scale increases would also be gradual[1].

Such extensive real world testing is necessary before the system going live at scale on a full state election, yet local and overseas experience is that testing and fit for purpose assurance is abandoned when time frames are too tight and there are (inevitable) blowouts

[1]Progress through the pilot program depends on satisfying stringent criteria that evaluate the risks and results of testing and live trials against security, reliability and quality hurdles. Failures and vulnerabilities, particularly in live trials, would require further testing and trials to be added.

in build time. This is what happened with the existing iVote system for example, but also with the other main electronic voting systems internationally including those of Norway, Estonia, and Switzerland. Alarmingly even under the current optimistic roadmap for iVote there is only *one week* allocated for penetration testing (a key part of security testing) before going live, and insufficient time to respond if any non-trivial vulnerabilities are discovered. Of course any development blow-outs would further reduce that testing time.

In summary there is a non-negligible and foreseeable risk that using either the existing or proposed iVote systems for more than a small proportion of voters in the NSW 2019 State Election could lead to a perversion of electoral outcomes which may or may not be detected, public loss of confidence in the electoral system, in the NSW Electoral Commission, and to challenges to the legitimacy of candidates elected under the process.

Initially this risk was contained by carefully limiting the number of voters using the system. The first iVote was used on a small scale in 2011. This system was intended to accept in the order of 5000 votes[2], and this would have a reasonably low risk of failures affecting the election outcome even in a close election. Actual usage was an order of magnitude larger at over 46 000 votes[3]. Nevertheless the scale was still limited by restricting the categories of eligible voters. Carefully containing the risks of a new, unproven system was a sensible approach given the low system assurance and the live failures and vulnerabilities experienced, as well as actual usage far exceeding projected usage.

However this risk containment approach was subsequently abandoned and the second iVote was used on a large scale in 2015[4]. This system accepted over 283 000 votes[5], which is an even larger number than postal voting at its peak. Despite the problems experienced in 2011 and the use of another new, unproven system for 2015, a significant expansion of eligible voters was permitted. Again there was low system assurance and live failures and vulnerabilities were experienced but this time on a much larger scale. Again actual usage far exceeded projected usage. The plans for iVote 2019 propose yet another significant expansion of eligible voters and increase in scale for another substantially new, unproven system.

Consequently there is now increasingly rapid and unrestricted growth in the use of the highest risk voting methods in NSW elections. The combined use of iVote and postal voting was almost 11% in the 2015 State Election. Under the current plans it is conceivable that in 2019 the use of the highest risk voting methods could be over 20%.

In this submission we give selected examples of the problems we have identified in the existing iVote system and the new iVote system's Request for Proposal and Initiation Brief. These examples are intended to illustrate the main issues involved and the cultural

[2] This was well under one percent of the votes in the 2011 State Election.

[3] This was about one percent of the votes in the 2011 State Election.

[4] Although iVote 2015 was intended to have the capacity to accept 1 million votes, this is distinct from the appropriate level of usage based on the risks posed by problems with the system's security, reliability and/or quality. Also the actual capacity was much smaller: iVote 2015 experienced substantial performance failures in handling only 283 000 votes, and this delayed the counting by several days.

[5] This was 6.3% of the votes in the 2015 State Election.

change needed to address them, in response to the terms of reference of the iVote Inquiry. We have omitted entire categories of problems with the existing and new iVote systems due to time limitations. A comprehensive review is needed to identify and analyse all the problems that need to be remediated.

In the next section we make recommendations on the way forward for 2019 and 2023. Then we give examples of currently discovered problems with iVote. Finally we discuss what needs to be done to address the root causes of these problems.

2 Recommendations

Recommendation 1. *If iVote is used for the 2019 State Election then it should be used on a small scale for voters with disabilities and voters living in remote regions. This version and any future versions derived from any of its components should not be used in any subsequent election where the number of votes cast using the system could have a significant effect on the election outcome.*

The version of iVote used in 2019 should be based on the existing version and improvements should concentrate on transparency, scrutiny and assurance. No attempt should be made to replace existing working code with experimental code at this late stage. An independent security review and risk assessment should be carried out to identify and prioritise the security issues to be addressed in the existing code.

These measures will help to limit risks and to tighten the scope to concentrate on a narrower set of critical requirements by reducing/eliminating speculative requirements with limited immediate practical impact such as system flexibility (for instance for use in polling places and for running multiple elections simultaneously), performance and extensibility.

The single-use nature and reduced scope will also help to avoid the temptation to attempt to develop common components for 2019 and 2023. Under the current circumstances and time frame such additional complexity would substantially increase the risks for both 2019 and 2023.

Recommendation 2. *For elections subsequent to 2019 a new version of iVote should be developed based on an entirely new design and approach. The NSWEC (perhaps in conjunction with other electoral commissions) should oversee the creation of the high-level system design, including cryptographic protocols for registration, voting and verification. This version of iVote should be designed to be suitable for long-term large-scale use.*

A minimum of four years needs to be scheduled for developing the system so that there is adequate time to achieve reasonable system maturity and high assurance, including extensive testing and small-scale pilot deployments. This is assuming that the NSWEC has first built up sufficiently advanced technological capabilities.

The 2023 State Election is a feasible target provided that preparations begin now and the NSWEC has sufficient resources to carry out the work in parallel with any work on

iVote for 2019. The focus always needs to remain on 2023 and care must be taken to avoid work on iVote 2019 diverting resources from iVote 2023.

It is vital that NSW retains control over its electoral process and that the security design and system IP remain under its control rather than vendor control.

Recommendation 3. *Failure-critical engineering practices should be established and followed for the iVote system, which is critical national infrastructure. As a first step iVote needs*

1. *to have strong, specific, upfront requirements for security, reliability, quality, transparency and scrutiny; and*
2. *to be engineered to meet these requirements from the outset, and to enable high assurance that these critical requirements are satisfied.*

Recommendation 4. *The NSWEC should build and sustain advanced internal technological capability. As a first step this needs to include a sufficient number and range of specialists with the necessary expertise in failure-critical engineering, security, cryptography and risk.*

The NSWEC should immediately recruit sufficient specialists in these disciplines to work on key tasks including

- designing and implementing failure-critical engineering practices,
- sharing security and technological knowledge throughout the entire organisation,
- evaluating vendor proposals for iVote and other election technology, and
- providing rigorous oversight and governance of IT contractors and other external providers.

Recommendation 5. *Legislative, regulatory and/or administrative provisions should be updated to explicitly address and support transparency and scrutiny for Internet voting and election technology. The first steps are to introduce provisions*

1. *for transparency and scrutiny that are designed specifically for electronic systems;*
2. *to remove barriers to transparency and scrutiny, in particular conflicts of interests where commercial interests may override the public interest; and*
3. *to establish a security board of independent technical experts to provide oversight and support scrutiny of Internet voting, and to ensure public confidence in the outcomes of the systems used.*

3 Examples of iVote Problems

In this section we give examples of problems with security, transparency and scrutiny in the existing iVote system.

3.1 Problems with Security

The iVote system has vulnerabilities inherent in the design of each of its three components: the Credential Management System, the Core Voting System and the Verification Service.

In contrast to *implementation* vulnerabilities, the only effective way to mitigate such *design* vulnerabilities is to redesign the entire system from scratch. Attempting to bolt on an ongoing series of countermeasures to address exploits as they are discovered typically results in overly complex design and security measures that in practice are cumbersome and ineffective. Such countermeasures can also introduce other new vulnerabilities and cause more serious weaknesses (even extending to other areas including causing reduced reliability, transparency and scrutiny).

We give some examples of iVote design flaws that have created vulnerabilities in authentication, vote privacy and verifiability. These are in addition to previously published vulnerabilities. There are likely many more such vulnerabilities which have not yet been discovered (by us).

3.1.1 Authentication Vulnerability

An example of an iVote authentication vulnerability is that **an attacker can cast votes for registered voters without knowing any iVote Numbers or PINs**.

A voter's credential is a hash derived from the voter's iVote Number and PIN. When voting the browser submits this credential hash to authenticate the voter to the Core Voting System[6]. The Core Voting System has a credential list of all the voters' credential hashes, and checks that the submitted credential hash is in this list. An attacker (including an insider) who steals this list can simply use the credential hashes in the list to impersonate voters[7].

This vulnerability is caused by a design flaw in the way credentials are constructed and used, and is a symptom of fundamental design flaws in the Credential Management System[8]. Note this vulnerability is much more serious than the more obvious vulnerability caused by using only six-digit PINs, which are too short and thus result in weak credentials for impersonation.

[6] This is a nonstandard authentication method. The standard authentication method would be for the browser to send the username and password (iVote Number and PIN in this case), and then the server computes a hash of the password. The standard method was designed to avoid this type of vulnerability.

[7] Note that encrypting the credential list would not be an adequate countermeasure.

[8] While the Core Voting System assists in constructing credentials, the constraints are primarily due to the Credential Management System.

3.1.2 Vote Privacy Vulnerability

An example of an iVote vote privacy vulnerability is that **an attacker can break privacy of all the votes by compromising a single machine,** *learning how every voter voted.*

The Election Key for decrypting all the votes is split into key shares. The key shares are distributed to particular staff, with the intention that multiple staff must combine their key shares to decrypt the votes. The key shares are generated on a single machine and later combined on a single machine. An attacker who compromises this machine can then steal the Election Key to decrypt all the votes.

This vulnerability is a single point of failure design flaw where vote privacy relies entirely on a single machine remaining secure, with no protection if the machine is compromised. In practice a large number of people have the opportunity to compromise the machine: multiple people have authorised access to the machine, whilst others are able to gain (unauthorised) physical access to the machine (and thus could also compromise the machine).

Furthermore even when the machine has not been compromised there is no way for members of the public to know that this is the case. They can never be sure that nobody knows how they voted.

3.1.3 Verifiability Vulnerability

An example of an iVote verifiability vulnerability is that **votes can be changed by an attacker, a system failure or human error without being detected by voters**.

The Verification Service is intended to provide **recorded-as-cast** verifiability, which means that a voter can detect if their vote recorded (stored) in the Voting System has been changed (for instance by the Voting System). The Verification Service does allow voters to check their votes but not directly: since the Verification Service is separate from the Voting System, a voter is in fact checking an entirely separate copy of their vote and this copy they check is not the recorded vote used for counting. Consequently a voter cannot detect if their recorded vote has been changed by the Voting System or a subsequent process, and so iVote fails to provide recorded-as-cast verifiability.

The Verification Service has an additional feature for voters to check their Receipt Numbers after the votes are published. This is intended to enable voters to verify that their votes were counted, and some other Internet voting schemes do issue similar receipts to help provide recorded-as-cast verifiability. However in iVote the votes can be changed without changing Receipt Numbers, and so checking Receipt Numbers does not help detect such changes to votes.

This vulnerability is partly caused by a design flaw in the Verification Service from the first version of iVote in 2011. That version included the Receipt Number check in an attempt to provide some form of verifiability but it is not effective.

3.2 Problems with Transparency

The iVote system and project has numerous substantial transparency weaknesses caused by problems with the creation, management and openness of material needed to support transparency in complex IT systems. These transparency weaknesses have a wide range of well-known consequences including preventing scrutiny and oversight, undermining public confidence in the system and increasing the risk of unnoticed vulnerabilities and defects caused by human error, misunderstandings and miscommunications.

Problems with creating and managing material. Audits of iVote 2011 and iVote 2015 noted that key documents were incomplete, inconsistent, out-of-date, unorganised, created at the last minute or not created at all [PWC11a; PWC11b; PWC15].

Notably iVote does not have comprehensive and accurate documentation of the high-level design, how it satisfies the core requirements, and what assumptions are made. To help address this shortcoming, we[9] have been collaborating with the NSWEC to write this critical document. The work began in mid 2016 and is close to completion but recently has been put on hold as the iVote team has needed to switch focus to the next version of iVote.

Problems with openness of material. Very limited material is released for public and expert scrutiny and audit, or as evidence of iVote's properties and level of assurance (for instance assertions that iVote is secure are not accompanied by meaningful details on its security properties and how they are reviewed and tested). Moreover the released documents are published when it is too late to address problems that they may reveal.

Notably no source code is published, which is in contrast to the jurisdictions overseas that use large-scale Internet voting. As a result both public and expert scrutiny has been prevented by onerous confidential agreements [CORE12a].

3.3 Problems with Scrutiny

The iVote system has scrutiny weaknesses because the system and project to design and develop the system were not themselves designed for transparency and scrutiny from the outset. This has made it difficult to retrospectively create opportunities for effective scrutiny and oversight by candidates, political parties, the parliament, the public and experts. This has also made it difficult to ensure high assurance is provided through testing, review and audit.

Problems with scrutiny opportunities. The existing iVote does not have any scope for direct, meaningful scrutiny by candidates, political parties, the parliament, the public or experts.

For iVote 2015 a Decryption Ceremony was introduced where Independent Comparators conduct some scrutiny of the iVote data. However this covers only a small part of the system, and so the bulk of the system and processes remain invisible and are not subject to such scrutiny.

Furthermore the process for providing data to the Independent Comparators has not been designed to include chain-of-custody integrity checks (for instance digital signatures

[9] the two of us together with Professor Annabelle McIver and Professor Carroll Morgan

that can be verified by the Independent Comparators), and so there is no way to detect if the scrutiny is conducted on tampered data.

Scrutineers and political parties were allowed to attend the Decryption Ceremony and observe the Independent Comparators. While this was positive in engaging political parties with iVote, it did not allow them to actively perform any scrutiny.

Moreover the Independent Comparators are bound by confidentiality agreements with the NSWEC[10]. (This is due to an iVote design flaw where the comparison programs must be run on sensitive data that can reveal how voters voted.) An unintended consequence is that Independent Comparators are limited in their ability to report problems publicly, to scrutineers and to candidates: in practice the confidentiality agreements suppress the data needed to properly report, explain or independently verify problems (both during the ceremony and afterwards).

For example in the 2015 Decryption Ceremony our comparison program identified errors in over 3000 votes[11]. However it would have breached the confidentiality agreement to support scrutiny, for instance merely by showing scrutineers the raw data or error logs as evidence of the errors, or by providing scrutineers with the relevant vote details to facilitate independent verification, analysis and/or investigation of the errors. On this occasion the scrutineers and other observers simply accepted the NSWEC's explanation for the errors without asking for evidence or further details. But this current process cannot respond to more active, knowledgeable or analytical scrutineers.

Problems with assurance. Most of the known live failures that occurred in iVote in 2011 and 2015 can be attributed to insufficient time and expertise for testing, review, audit and remediation. For example previous and proposed future penetration testing for iVote is limited to the order of only one week in duration and is conducted by a general security consulting firm without the specialist expertise needed for the security issues particular to Internet voting. This basic level of security testing provides low assurance that failures, vulnerabilities and weaknesses are identified and properly addressed.

To increase the level of assurance and thus reduce the risk of repeating live failures again in 2019, the assurance plans need to be revised so that penetration testing and other such critical assurance activities are each scheduled to take in the order of months rather than weeks. (For making incremental improvements to the existing iVote system, this is an appropriate amount of time for assurance activities. But for developing a substantially new system as is the case with the current iVote proposal, substantially more time would be needed for assurance activities.) In addition assurance activities need to be scheduled as ongoing activities and allow ample time for issues to be detected, remediated and retested.

[10] The agreement requires the data supplied by the NSWEC to be kept confidential and prohibits Independent Comparators from copying or retaining this data. We had to seek legal advice to negotiate our confidentiality agreement to allow some data logged by our comparison program to be saved by the NSWEC and later returned to us. However log data containing information on individual votes, for instance in detailed error logs, was not allowed to be saved.

[11] Note that the NSWEC reference comparator and the other Independent Comparator failed to identify these errors. In the event of disputes the confidentiality agreement would have prevented the critical details of the disputed errors from being independently preserved. Fortunately in this case the NSWEC quickly acknowledged the errors.

4 Addressing the Root Causes

In this section we describe some of the changes needed to address the root causes of the above problems with iVote: establishing failure-critical engineering practices, building advanced internal technological capability, and implementing transparency and scrutiny provisions that support election technology. Much of this requires cultural change to transform the NSWEC into a world-class electronic voting organisation with the capability to effectively develop and operate critical national infrastructure.

4.1 The Need for Failure-Critical Engineering Practices

Failure-critical engineering practices are necessary for electronic voting systems, which are critical national infrastructure. We have written extensively on how many of the problems with iVote and election technology in Australia have been caused by following the much lower standard of best-effort commercial practices, which are susceptible to well-known risks of failures in IT systems and projects [BTW11; CORE12b; WB16; WB15; CORE11].

Some of the key principles of failure-critical engineering practices include

- **security, reliability and quality *by design.*** Key security, reliability and quality requirements are specified in detail upfront. These requirements are then central in developing the initial design rather than attempting to be later retrofitted to the design, which is usually highly problematic and ineffective.

- **transparency and scrutiny *by design.*** Upfront consideration, planning and commitment is given to what requirements are necessary to provide strong transparency and strong scrutiny. This includes specific, detailed transparency and scrutiny requirements for how the system must be designed and what material needs to be created and released (for instance documentation, third party reports, source code and software artefacts).

- **assurance *by design.*** Adequate time and resources need to be allocated for ongoing assurance activities from the outset of the project, including testing, review and audit. A common problem is that assurance activities are scheduled for short periods towards the end of the project, often in ambitious schedules that have short time frames and are high susceptibility to delays. This has a high risk that issues will not be identified or addressed in time, that inappropriate shortcuts will be taken to defer or drop certain assurance activities, and that irreversible commitments will result in the decision to still use iVote despite serious risks or problems being discovered.

- **risk focus.** Risk management is integrated into all engineering, management and decision-making processes. In particular risk assessments are genuine rather than being compliance exercises, and are comprehensive and ongoing so that serious risks are properly identified, evaluated and mitigated.

- **continuous improvement over basic compliance.** Continuous improvement is planned and driven by ongoing reviews and audits of the engineering and project practices. Also lessons learned are immediately put into practice to avoid repeating the same mistakes.

4.2 The Need for Advanced Internal Technological Capability

Electoral commissions running electronic elections need to build up advanced internal technological capability to ensure the security, reliability, quality, transparency and scrutiny of electronic election systems.

In many respects electronic voting systems and other election systems have more complex and sophisticated requirements, risks and features than banking and military applications. To retain full control of the development and operation of these systems (even when third parties are involved), a broad range of highly specialised expertise is essential. For example identifying, analysing and addressing the immense number and diversity of security issues requires a dedicated team of security specialists from the outset. This security team must be carefully chosen so that their combined expertise covers all key security areas.

At present electoral commissions in Australia have very limited technological capability. For example the iVote team does not have a sufficient number and range of specialists with the necessary expertise in core disciplines such as failure-critical engineering, security, cryptography and risk. Some external expertise is engaged to cover some of the gaps but only for short periods and largely late in the project cycle.

Some examples of activities where specialist expertise is essential are

- **developing failure-critical engineering practices.** Compliance with basic commercial practices is the usual approach because familiarity with rigorous engineering practices is not common. For example planning and practices for security assurance in commercial systems are often severely inadequate.

- **developing and evaluating high-level designs.** Fundamental design flaws are common in electronic voting systems. In particular security and cryptography design flaws can be notoriously difficult to prevent and detect, and "roll your own cryptography" is highly prone to being broken.

- **understanding security properties, security standards, cryptography and electronic voting designs.** Frequent misconceptions are caused by the high complexity in these areas. Common problems include incorrect claims about a system's security properties; incorrect application of security standards; incorrect or unnecessary use of cryptography; and incorrect analysis and comparisons of different cryptographic techniques and design approaches for electronic voting systems.

- **providing rigorous oversight of electronic voting vendors and other providers.** Rigorous oversight is problematic because electoral commissions are heavily dependent on external technology providers. For example vendors are relied

upon to respond to expert criticism of vulnerabilities and weaknesses in electronic voting systems, and this has included vendor submissions to parliamentary inquiries. This dependency also creates a power imbalance for vendors over electoral commissions. For example vendors are frequently depended on to determine what the critical requirements should be (in line with their own solutions!) rather than being given firm, binding requirements that must be satisfied. This has even extended to transparency requirements and has allowed electronic voting vendors to create barriers to transparency [CORE12a] which operate in their own interest rather than the public or national interest.

4.3 The Need for Transparency and Scrutiny Provisions for Election Technology

Elections in NSW need legislative, regulatory and/or administrative provisions that explicitly address and support the complex transparency and scrutiny issues accompanying the use of electronic voting and other technology in modern elections.

Overseas jurisdictions using electronic voting (Switzerland, Estonia and Norway) are considerably advanced in implementing legislative, regulatory and administrative provisions designed to support effective and safe electronic voting systems and this has led to much stronger transparency, scrutiny and oversight than currently exists in Australia. Despite using electronic voting *on an even larger scale* than these jurisdictions, NSW has yet to explicitly and publicly consider what provisions are necessary to support transparency, scrutiny and oversight, as well as remove current barriers.

Some of the key elements which need explicit support in this new way of conducting elections include

- **explicit support for strong and enforced transparency.** Overseas jurisdictions have developed strong and enforced transparency provisions for electronic voting, which mandate not only publishing the source code but also publishing other material including project and technical documentation, third party reports, software artefacts, vendor contracts and even videos of vendor presentations. Such mandates ensure that plans and commitments for transparency are binding, high-priority, specified in detail, and made upfront. Furthermore mandated transparency has helped overcome barriers to transparency caused by conflicting interests such as external vendors wishing to limit openness to maximise their commercial advantage in keeping source code secret.
  In the absence of such provisions in NSW and Australia, transparency of election technology is voluntary and in many instances barriers have arisen. In particular commercial interests have had substantial influence in setting a low level of transparency for election technology. It is important to note that vendors have been willing to comply with the strong transparency mandates described above when bidding for electronic voting tenders in overseas jurisdictions, but they have successfully avoided such transparency measures in NSW. Even Australian parliaments have been unable to overcome such barriers created by commercial interests.

For example the Federal Senate failed to compel the AEC to publish the source code for the EasyCount Senate vote counting software. The AEC successfully argued that the software was commercial-in-confidence because it was also used for fee-for-service elections.

- **provisions for oversight by independent technology experts.** All overseas jurisdictions using Internet voting have mandated oversight by independent technology experts. Estonia and Norway have External Technology Boards. In Switzerland the Federal Chancellery has internal technological expertise to provide oversight of the cantonal (state level) electronic voting systems[12]. This rigorous external oversight of electronic voting is one of the strongest drivers of continuous improvement and has helped to deliver these electronic voting systems with higher levels of security, quality and public confidence. The absence of such oversight in Australia has contributed to the persistence of systemic issues in electronic voting systems.

- **provisions for scrutineers and candidates.** In Australia provisions that are introduced to allow the use of electronic election systems do not include appropriate safeguards for meaningful scrutiny. As a result scrutiny of electronic systems by scrutineers remains limited to observation of physical artefacts and processes in the same way as scrutiny of manual systems, even though such observation on its own can be meaningless for scrutiny of election technology — simply watching a computer screen and possibly asking some questions is highly unlikely to reveal technical problems or counting errors.

  In the absence of explicit provisions that have been carefully designed to support and create opportunities for effective scrutiny of electronic systems, barriers to scrutiny have arisen. For example in the 2016 Federal Election, a scrutineer requesting material needed to effectively scrutinise the Senate vote capture system was denied on the basis that the Commonwealth Electoral Act did not include specific provisions to allow this [BBWR16].

  In addition although technology has become pervasive in conducting elections, scrutineers and candidates still have no effective mechanism to raise concerns over scrutiny issues, irregularities and failures in election technology. This can undermine trust in both election integrity and dispute resolution provisions, as demonstrated in technological controversies in US elections such as the recount petitions in the 2016 US Presidential Election.

References

[BBWR16] Ian Brightwell, Richard Buckland, Roland Wen and Clancy Rye. *Questions on Notice — Public Hearing 16 November 2016. Supplementary Submission to the Inquiry into and report on all aspects of the conduct of the 2016*

[12] All Swiss elections are run by the cantons.

Federal Election and matters related thereto. Submission 56.1, Inquiry into and report on all aspects of the conduct of the 2016 Federal Election and matters related thereto. Joint Standing Committee on Electoral Matters, Parliament of Australia, 2016.
URL: http://www.aph.gov.au/DocumentStore.ashx?id=44eac9f0-f3fe-47cc-84e1-d34453285981&subId=459558.

[BTW11] Richard Buckland, Vanessa Teague and Roland Wen. "Towards Best Practice for E-election Systems - Lessons from Trial and Error in Australian Elections". In: *E-Voting and Identity - Third International Conference, VoteID 2011, Tallinn, Estonia, September 28-30, 2011, Revised Selected Papers*. Ed. by Aggelos Kiayias and Helger Lipmaa. Vol. 7187. Lecture Notes in Computer Science. Springer, 2011, pp. 224–241.
URL: http://dx.doi.org/10.1007/978-3-642-32747-6_14.

[CORE11] Roland Wen, Vanessa Teague and Richard Buckland. *Best Practices for E-election Systems. Computing Research and Education Association of Australasia (CORE) Supplementary Submission to the Inquiry into the 2010 Federal Election*. Submission 101.1, Inquiry into the 2010 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia, 2011.
URL: https://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=em/elect10/subs/sub101.1.pdf.

[CORE12a] Vanessa Teague and Roland Wen. *Computing Research and Education Association of Australasia (CORE) Supplementary Submission to NSW JSCEM*. Answers to Questions on Notice, Inquiry into the Administration of the 2011 NSW election and related matters. Joint Standing Committee on Electoral Matters, Parliament of NSW, 2012.
URL: https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryOther/Transcript/6720/Answer%20to%20QONs%20-%20CORE%20(28062012).pdf.

[CORE12b] Vanessa Teague and Roland Wen. *Problems with the iVote Internet Voting System. Computing Research and Education Association of Australasia (CORE) Submission to the Inquiry into the Administration of the 2011 NSW Election and Related Matters*. Submission 7, Inquiry into the Administration of the 2011 NSW election and related matters. Joint Standing Committee on Electoral Matters, Parliament of NSW, 2012.
URL: http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/BA09355EDE5E3859CA2579AD0001D53C.

[PWC11a] PWC. *Technology Assisted Voting Audit — iVote Post Implementation Report*. 21st June 2011.

[PWC11b] PWC. *Technology Assisted Voting Audit — iVote Pre Implementation Report*. 7th Mar. 2011.

[PWC15] PWC. *Post Implementation Review of the iVote Project*. July 2015.

[WB15] Roland Wen and Richard Buckland. *Problems with E-Voting in the 2014 Victorian State Election and Recommendations for Future Elections*. Submission 12, Inquiry into the Conduct of the 2014 Victorian State Election. Electoral Matters Comittee, Parliament of Victoria, 2015.
URL: http://www.parliament.vic.gov.au/images/stories/committees/emc/2014_Election/Submissions/No_12_Dr_Roland_Wen_and_Associate_Professor_Richard_Buckland.pdf.

[WB16] Roland Wen and Richard Buckland. *Submission to the Victorian Inquiry into Electronic Voting*. Submission 23, Inquiry into Electronic Voting. Electoral Matters Comittee, Parliament of Victoria, 2016.
URL: http://www.parliament.vic.gov.au/images/stories/committees/emc/Inquiry_into_Electronic_Voting/Submissions/No_23_Dr_Roland_Wen_and_Associate_Professor_Richard_Buckland.pdf.