Received: September 2, Date of acceptance: October 16, 2020, Date of publication: November 9 2020, DOI: https://doi.org/10.26826/law-in-context.v37i1.119

Electronic Australian Elections: Verifiability of Accuracy is a Design Goal, which Must be Mandated by Law and Deliberately Designed into Electronic Electoral Processes

By **Vanessa Teague**[1], **Orcid:** *https://orcid.org/0000-0003-2648-2565*

and **Patrick Keyzer**[2]**,** Research Professor of Law and Public Policy at La Trobe University, **Orcid:** *https://orcid.org/0000-0003-0807-8366*

[1] Thinking Cybersecurity Pty Ltd and the Australian National University

[2] La Trobe University

ABSTRACT

Electronic voting and counting are increasingly common and have been adopted in a number of Australian jurisdictions. Unfortunately, there is evidence that e-voting systems lack transparency. At present there are reasonable solutions for poll-site e-voting but none for remote paperless Internet voting. Although there are reasonable methods for statistical audits of electronically counted election results, Australian elections do not use them. The authors argue that a purposive approach should be taken to relevant electoral laws to ensure that genuine scrutiny of electronic electoral processes can be undertaken. This would require the source code and the voting data to be made available for testing. The authors recommend a number of legislative reforms to ensure the verifiability of e-voting. These reforms need to be undertaken to ensure that Australian elections are accurate, and consistent with the constitutional requirement of direct choice by electors.

Keywords – *Elections, electronic voting, scrutiny, security, verifiability*

Acknowledgments – *We thank Associate Professor Jeffrey Barnes and Mr Joel Butler for their helpful comments on previous drafts.*

Disclosure statement – *Vanessa Teague has engaged in several consulting projects with the Swiss Federal Chancellery, to examine their e-voting system and advise on their regulations. She is also on the board of advisors of Verified Voting. No potential conflict of interest was reported by Patrick Keyzer.*

Suggested citation: Teague, V. and Keyzer, P., “Engineering Australian Elections: Verifiability is a design goal, which must be mandated by law and deliberately designed into electronic electoral processes” *Law in Context,* 37 (1): 42-65. DOI: https://doi.org/10.26826/law-in-context.v37i1.119

Summary

1. INTRODUCTION: THE UNCHANGING REQUIREMENTS OF ELECTORAL PROCESSES

Australians have been engineering better electoral processes for over one hundred and sixty years. In 1856, the colony of Victoria, newly separated from New South Wales, was defining the rules for its first election, which commenced on the 23rd of September that year (Brent 2006; Chapman 1967).

> *William Nicholson, a Member of the Legislative Council, moved in late 1855 that the elections be conducted by secret ballot. It would prevent voter intimidation, he argued, particularly by the government, which was a very large employer; and it would stop the practice of "treating" and hence make elections more orderly (Brett 2019; see also Hasen 2000).*

Henry Chapman, another member of the Legislative Council then designed the new system: voters had their names marked off on an electoral roll at a polling place, were presented with a printed ballot paper, and retired to separated stalls to mark their ballot paper, in secret, before depositing their ballot paper in a locked box under the watchful eye of a poll clerk (Sawer 2010). By the time the Victorian election took place, Tasmania and South Australia had followed suit (Brent 2006; Newman 2003). The use of voting stalls

> was just as crucial to the success of the scheme as the ballot paper. Together, these practical measures made secret voting a workable reality (Brent 2006).

These electoral processes were deliberately designed with specific security goals in mind, and these designs and requirements were written into law.

Different countries devised different solutions to achieve the same goals. For example, French voters put their (candidate-coloured) ballot paper into an envelope before depositing it in a transparent urn (Balinski and Laraki 2010). Some jurisdictions, particularly some parts of the United States, have never adopted secure and transparent electoral processes, and have suffered decades of troubled elections as a result (Gumbel 2005; Jones and Simons 2012).

There are two main election security requirements:

Ballot Secrecy

Nobody, including administrators, should be able to link a voter to their vote. This protects voters from vote-buying and coercion.

Transparency

It should be possible for observers to verify that the election is conducted properly through scrutiny, removing opportunities for undetectable error or fraud.

These goals are as critical now as they were in 1855.

The first aim of this article is to tease out contemporary challenges to the transparency of elections in Australia, particularly relating to electronic electoral processes. Australian State and Territory and also Commonwealth electoral laws all contemplate scrutiny. (See for example *Commonwealth Electoral Act* 1918, Part XVIII; *Electoral Act* 1992 (ACT), ss 122-3; *Electoral Act* 2017 (NSW), Division 7 and s 158 (analysed below); *Electoral Act* 2004 (NT), ss 46-7, 128 and Div 5 subdiv 2; *Electoral Act* 1992 (Qld), s 104; *Electoral Act* 1985 (SA), s 67 and Part 10 (note Div 3A, which addressed "Computer vote counting in Legislative Council elections"; *Electoral Act* 2004 (Tas), Parts 5 and 11, and s 172; *Electoral Act* 2002 (Vic), ss 76, 110, 111, 114, 116 and 119; *Electoral Act* 1907 (WA), ss 92, 99, 117, 134, 137, 144-6). But in general these laws have been written having regard to the technology of the time, *i.e.*, when standing in a room and watching what was going on was sufficient to ensure the process was running properly. Increasingly, Australian electoral processes are electronic. In this article we demonstrate that electoral law and practice has not evolved to achieve the crucial objective of meaningful scrutiny of electronic electoral processes. If anything, we have gone backwards.

The second aim of this essay is to describe the most important reforms that are required to ensure that our electoral law is consistent with the principles of the secret ballot and meaningful candidate-appointed scrutiny, when a large part of the electoral process is electronic. Drawing upon successful examples of good regulation in other democracies, we will explain the highest reform priorities for Australia's electoral law. We demonstrate below that these reforms are urgently needed when recent developments are taken into account – the Australian Electoral Commission recently argued that even the existing, very basic, scrutineering provisions did not apply to those parts of the electronic Senate counting process they had outsourced. Finally, we provide a plan for what changes need to be made to achieve ballot secrecy, transparency and accuracy.

2. THE MANY ROLES OF COMPUTERS IN AUSTRALIAN ELECTIONS

2.1 MANY EXPERIMENTS AND NO CONSENSUS

Australia has nine electoral systems; one for each of the Commonwealth, the States and the two self-governing territories. (A tenth electoral jurisdiction, Norfolk Island, operated as a self-governing Territory between 1979 and 2015. See the *Norfolk Island Act* 1979 (Cth) (repealed), and the *Norfolk Island Legislation Amendment Act* 2015, and, further, O'Collins 2002). The nine polities have conducted interesting experiments in elections from time-to-time. They each have subtly different, but also broadly similar laws and practices.

That said, there is very little logic or consistency in the use of computers across Australia's electoral commissions. For example, consider the electronic counting of the Single Transferable Vote (STV) (Tudeman 1995). For this very complex vote-counting function, counting by computer has numerous obvious advantages. Unsurprisingly, many electoral commissions, including the Australian Electoral Commission (AEC) (for counting the Senate), most of the States (for counting their Legislative Councils) and the Australian Capital Territory (for its unicameral Legislative Assembly) implement some form of electronic counting of STVs.

Publication of the source code and the voting data is the minimum necessary for enabling public error-checking of processes and results of electronic electoral processes. The Australian Capital Territory Electoral Commission publishes both the source code and the voting data, so interested parties can use the official code to rerun the count themselves (at least it did until this year – see Elections ACT "Electronic voting and counting", accessed 20 August 2020, discussed further in Section 3.4). The Victorian Electoral Commission publishes the source code, but not the voting data, citing vote privacy concerns. This makes it possible to examine the official code for errors, but not to double-check the count itself. The AEC publishes the vote data but has refused specific requests to release the code, citing security concerns and also the protection of information that is considered to be "commercial-in-confidence" (see Section 3.3). The New South Wales Electoral Commission (NSWEC) is similar. West Australians can observe neither code nor data. Although there are academic projects that provide a general framework incorporating various options for STV counting, (Ghale et al 2018) neither a shared software project nor a unified national approach to verifiability (and therefore transparency) seem likely.

Voting by computer varies even more widely. Western Australia and South Australia have conducted small experiments allowing computer-assisted completion of a paper ballot in a polling place for voters with disabilities. The Australian Capital Territory has had electronic voting in a polling place (in which the actual vote is electronic) for many years, and both New South Wales and Victoria have provided this also. Victoria briefly experimented with an end-to-end verifiable electronic voting system for use in a controlled environment (such as an embassy or consulate) by voters living abroad. The NSW Electoral Commission uses its iVote Internet voting system, which in the 2015 and 2019 elections received more than 200,000 votes. They have tried to market it to other commissions, but so far only WA has adopted it, and on a much more limited scale.

So we have a number of experiments, but no consensus. Neither the requirements (for privacy, transparency, security, etc) nor even the basic question of what constitutes an acceptable level of risk, are broadly agreed across Australia.

Except possibly electronically-assisted completion of a paper ballot, none of these systems truly replicate the scrutiny opportunities of a traditional polling place. Even if both the source code and vote data are available, scrutineers still need evidence that the electronic votes accurately reflect the voters' intentions. This may fail for numerous reasons, even if the electoral commission has published a record of the votes and advertised code that seems to be correct: there could be malware on the machines that saves a vote different from the one that the voter asked for, or there could be a configuration problem that swaps two candidates' positions on the touchscreen, or there could be a problem with the communication of results that causes some of them to be dropped in transit, or many other similar problems. There is not necessarily any way for scrutineers to detect any of these problems, even if they are standing at the polling place. This applies both to electronic counting systems, where we need to check that the electronic vote data accurately digitizes a paper ballot, and to electronic voting systems, where we somehow need to solve the much harder problem of verifying that an electronically-captured vote accurately reflects the voter's intention.

Verifying the entire data flow, from voter intention to election outcome, is the subject of the next section.

2.2 VERIFIABILITY IS A DESIGN GOAL THAT SHOULD BE LEGISLATED

The purpose of scrutiny in an election is to allow the representatives of candidates (scrutineers) to verify that the election has been conducted fairly and properly.

There are two main ways to ensure proper scrutiny in an electronic process. The first, described in Section 3, is to examine the software, specifically the source code and related documentation, to understand how the system is intended to work. This should specify, in precise detail, exactly what computations are being performed and what protections are in place. This is a good way of checking for accidental errors or security problems (and many have been found, as we shall demonstrate below).

That said, examination of the source code and related documentation does not really prove whether the election was properly conducted on the day. For one thing, a corrupt insider or external attacker could simply cause different software to run on the real election system on election day. This insight has motivated many years of technical research into the question of how one could verify an election result without trusting the electronic system on which the election was conducted.

It is very important to understand that verifiability does not come automatically – naively designed electronic systems may be subject to fraud that is undetectable by human observers. Just as paper-based processes need to be designed with observability in mind—we do not let our electoral commissions count paper votes in secret, away from the eyes of scrutineers—electronic ones need to be designed to generate evidence that they have correctly handled the votes. The slogan must be ‘verify the election, not the software.’ Successful examples, and important failures, are described in Section 4.

The main idea we want to convey in this essay is this: *Verifiability is a design goal, which must be mandated by law and deliberately designed into electronic electoral processes.*

We strongly support both the open availability of the software *and* the verifiability of the process. Although in theory you could have one without the other, they are complementary and both contribute substantially to evidence that the system functions appropriately and achieves what we want elections to achieve: demonstrated accuracy. For one thing, it seems hard in practice to convince anyone that the verification process is sound without revealing details of how it works.

2.3 THE STRUCTURE OF THIS PAPER

In Section 3.1, the next section of this article, we will explain the verifiability failures discovered in the SwissPost Internet voting system. This provides a case study that we use as a reference point. Then, in Section 3.2, we will consider the implications of identical errors in the NSW iVote system. The question of the availability of the counting code in Australian Senate elections is considered in Section 3.3. In Section 3.4 we will critically evaluate the ACT's EVACS system.

For each of these examples, we’ll describe what can be learned by examining the software, then discuss in Section 4 how (or whether) the system provides adequate evidence to verify its outcomes and, where possible, explain how it could be reformed to do so. In particular, through an analysis of the relevant provisions of the NSW *Electoral Act*, we will demonstrate that provisions regulating audits, monitoring and scrutiny of electronic electoral processes cannot produce the required transparency. We argue that if we cannot feel confident that our electronic voting systems have not been compromised, then this raises not only cryptographic concerns, but quite possibly constitutional concerns.

In the final section of the paper we outline a plan for what changes need to be made to electronic voting in Australia to achieve ballot secrecy, transparency and accuracy.

3. SCRUTINISING THE SOFTWARE AND PROCESSES

This section examines what can be achieved by examining the source code, specifications and other documentation available for genuinely independent and open review. These activities make it possible to find errors and to understand more accurately what a system's security properties truly are. It is not, however, sufficient for the verification of the result (more on this later).

3.1. SWITZERLAND: HOW GOOD REGULATIONS CAN EXPOSE SERIOUS PROBLEMS

Switzerland has one of the oldest Internet voting projects in the world (Serdult et al 2014; Lust 2018). Although elections are administered by cantons, the Federal Chancellery administers standards and certification for Internet voting. Their regulations are strict, detailed, and emphasise privacy, verifiability and transparency (Barrat I Steve, Goldsmith and Turner, 2012). Openness of the source code is required. Modalities for publishing the source code include:

1. The source code must be prepared and documented according to the best practices.
2. It must be easily obtainable, free of charge, on the internet.
3. The documentation on the system and its operation must explain the relevance of the individual components of the source code for the security of electronic voting. The documentation must be published along with the source code.
4. Anyone is entitled to examine, modify, compile and execute the source code for ideational purposes, and to write and publish studies thereon (*Verordnung der BK über die elektronische Stimmabgabe* (VEleS) [Federal Chancellery Ordinance on Electronic Voting (VEleS)] (Switzerland) 13 December 2013 SR 161.116 art 7b).

However, this requirement applies only to software seeking certification for use by up to 100% of voters. Certification for use by up to 50% of voters can be achieved by software that is not openly available for public scrutiny.

In early 2019 with a team of other researchers, one of us examined the source code made available to comply with that regulation (Lewis, Pereira and Teague 2020). Three serious cryptographic errors were found. It was independently demonstrated that the first two could be exploited to forge a cryptographic 'proof' that the electronic votes had been correctly shuffled and decrypted, when actually other votes had been substituted (Haines et al 2020). Crucially, this proved that the system did not meet the verifiability criterion necessary for certification for use by up to 100% of voters.

> *For universal verification, auditors receive proof that the result has been ascertained correctly. They must evaluate the proof in an observable procedure. To do this, they must use technical aids that are independent of and isolated from the rest of the system. The proof must confirm that the result ascertained:*
>
> *(a) takes account of all votes cast in conformity with the system that were registered by the trustworthy part of the system;*
>
> *(b) takes account only of votes cast in conformity with the system;*
>
> *(c) takes account of all partial votes in accordance with the proof generated in the course of the individual verification (Verordnung der BK über die elektronische Stimmabgabe (VEleS) [Federal Chancellery Ordinance on Electronic Voting (VEleS)] (Switzerland) 13 December 2013 SR 161.116 art 9, Annex, art 5.4).*

These first two discoveries did not overly concern the Swiss, because the whole purpose of open and public scrutiny had been to identify and correct errors of this kind. However, the third problem affected a property called 'individual verifiability.'

> *For the purpose of individual verification, voters must receive proof that the server system has registered the vote as it was entered by the voter on the user platform as being in conformity with the system. Proof of correct*

> *registration must be provided for each partial vote (ibid., Art 4.2). Unlike the earlier errors, this problem also affected an earlier system already in use and already certified for use by up to 50% of voters. It allowed malware on the voter's computer to produce a 'proof' that allowed for apparently-valid vote verification for the voter, while actually submitting a nonsense vote that would not be counted. This was a far more serious matter for the Swiss, because it indicated that an already-certified system did not meet its certification standards, which in turn demonstrated that their non-public certification process had failed.*

Internet voting in Switzerland has been on hold since these discoveries, while the system designers attempt to repair their cryptographic protocol and the Chancellery tightens their regulations further. There has been considerable public discussion and debate about these errors and their implications for the future of Internet voting in Switzerland (Federal Council of the Swiss Confederation, 2019). The main point is that well-written *regulations* that emphasise transparency brought serious technical problems to light. The clear definitions of the required security properties allowed researchers to demonstrate unequivocally that the system did not meet those requirements. If the earlier system had been made available for completely open public scrutiny earlier (rather than being the product of a closed certification process) it is much more likely that its errors would have been detected earlier.

3.2 INADEQUATE LAWS LEFT THE SAME PROBLEMS HIDDEN IN NEW SOUTH WALES

Election software is a global business. The Swiss e-voting system was provided by a multinational corporation, Scytl, which also provides the NSW iVote Internet voting system. Though the electoral systems and user experiences are quite different between countries, these two systems shared the same back-end code for shuffling and decrypting the votes. When the first of the weaknesses we found in the Swiss system was made public, the NSW Electoral Commission announced that their system was affected by the same problem (NSW Electoral Commission, 2019). This was March 12th, 2019. The important difference was that Switzerland was opening a system to scrutiny that they were considering using six months in the future; NSW was already running it for early voting, had already received votes, and was intending to decrypt on election day, March 23rd, 2019 (see NSW Electoral Commission, *Report on the Conduct of the 2019 NSW State Election*). In its report, the NSW Electoral Commission briefly remarked:

> *unlike the Swiss Post system, the machine on which the iVote mixnet runs was not physically connected to any other computer systems either within or outside the Electoral Commission. The mixnet issue was assessed and rectified before the relevant code was used for the 2019 NSW State election.*

The phrase "not physically connected" is a peculiar one. PWC's audit report, which is redacted, says "**** on air-gapped (offline) computers was not disabled" (PWC 2019). While one can only speculate on the identity of a word that has been redacted, it is possible that the word was "WiFi". This conclusion is reinforced by the use of the word "was" in the sentence. If that is so, then it is conceivable that the data could have been corrupted by an external party. (Internet connectivity is not necessary for insiders to manipulate the votes.) We may never know.

How did such a fundamental problem, so obvious to an expert observer that two other research groups independently discovered it in Switzerland, escape notice completely in NSW? We believe that NSW electoral law helps create this problem. While the 2017 *Electoral Act* contains provisions that appear to provide for auditing, monitoring and scrutiny of electronic electoral processes, they ultimately fail to provide the proper preconditions for *effective* auditing, monitoring and scrutiny.

We can start with s 156 of the *Electoral Act 2017* (NSW), which states:

156 INDEPENDENT AUDITING OF TECHNOLOGY ASSISTED VOTING

(1) The Electoral Commissioner is to engage an independent person (the "independent auditor") to conduct audits of the information technology used under the approved procedures.

(2) Audits under this section are to be conducted and the results of those audits are to be provided to the Electoral Commissioner:

(a) at least 7 days before voting commences in each Assembly general election at which technology assisted voting is to be available, and

(b) within 60 days after the return of the writs for each Assembly general election at which technology assisted voting was available.

(3) Without limiting the content of the audit, the independent auditor is to determine whether test votes cast in accordance with the approved procedures were accurately reflected in the corresponding test ballot papers produced under those procedures.

(4) The independent auditor may make recommendations to the Electoral Commissioner to reduce or eliminate any risks that could affect the security, accuracy or secrecy of voting in accordance with the approved procedures.

At first glance, the provision seems fit for purpose. The provision requires compulsory audits, before and after elections, by an independent person (more on this later), within specified time limits. By implication, the auditor may make recommendations relating to the "security, accuracy or secrecy of voting" (s 156(4)). The auditing *could* involve testing of source code, for example, because that would arguably fall within the expression "information technology" in s 156(1) and the implied objectives of the audit (as we will demonstrate below). The auditor has to provide the results of the audit to the Electoral Commissioner, and this report *could* be disclosed under NSW freedom of information legislation (the *Government Information (Public Access) Act 2009* (NSW) (more on this below).

Section 156 is, however, defective in material respects. There is no requirement that the auditor have suitable knowledge and technical expertise (a point we return to later). Knowing the right questions to ask is important. The audit may not include analysis of the source code or other relevant data. In addition, s 156 does not require that any particular tests be conducted. This means that tests that are critical and necessary to expose flaws with the system may not be conducted, making the "audit" meaningless.

Furthermore, the auditor's report is not public, but only made to the Commissioner. A request for information under freedom of information law, while conceivable, is unlikely to be approved. When introducing the iVote system in 2010, the NSW Government said (NSW Hansard, 24 November 2010):

> *schedule 3 of this bill will amend the Government Information (Public Access) Act 2009 to protect sensitive information kept for the administration of elections, including software programs and codes for the iVote system. The bill will amend the Government Information (Public Access) Act 2009 to provide for a conclusive presumption of overriding public interest against disclosure in relation to certain provisions in the Act, specifically those concerning secrecy relating to technology-assisted voting*...

We acknowledge that the auditor is intended to be "independent" but if the report need not be made public and cannot be disclosed via freedom of information laws, then it is impossible to effectively review the auditor's work. The auditor's appointment is not characterized by the type of tenure that is typically associated with an independent public official (contrast Schedule 2 of the Auditor-General Act 1997 (Cth)). The NSW Auditor-General, by way of contrast, holds office for a period of eight years (*Public Finance and Audit Act* 1983 (NSW), s 28).

How has section 156 worked in practice? Before and after the 2019 problems were detected, a number of internal audits failed to find serious cryptographic errors. The second of SwissPosts's three cryptographic problems was made public very near to NSW election day. The problem allowed the decryption service to fake a proof that the votes had been properly decrypted, while actually substituting nonsense votes that would not be counted. This time, NSWEC put out a press release claiming that the problem was 'not relevant' to the iVote system. This was implausible since the two errors affected the same part of the code (the mixing and decryption service). But since the source code remained secret, there was no way to test this claim.

Does section 157 improve upon s 156? Section 157 states:

157 INDEPENDENT MONITORING OF TECHNOLOGY ASSISTED VOTING

(1) The Electoral Commissioner may appoint one or more independent persons (an "independent monitor") to

monitor and observe the technology assisted voting process at an election, including the counting of votes cast by means of technology assisted voting and the general operation of the technology assisted voting process.

(2) An independent monitor is to report and may make recommendations to the Electoral Commissioner regarding the technology assisted voting process.

The first point to make about this provision is that it confers a discretion on the Electoral Commissioner. Strictly speaking, that means that the Commissioner need not exercise their power to appoint an independent monitor for the purposes of the provision. Assuming that an appointment is made, s 157 goes further than s 156, because it covers "the general operation of the technology assisted voting process" (s 157(1)). There is provision for a report under s 157, an accountability measure that is not stipulated by s 156.

"Monitoring" goes beyond merely "observing". "Monitoring" is also a verb that denotes systematic and ongoing review, and implies that there is something to monitor, but in practice it may not require more than observing what has been done. There is no indication in the provision what standards would be applied within the monitoring. Although possible, there is no indication that monitoring would require any testing, let alone the tests that cryptographers might apply to ensure the voting was accurate.

Like s 156, s 157 only requires the report to be given to the Electoral Commissioner. There is no requirement of tabling in Parliament, which would provide Westminster-style checks and balances (such as they are). There is no requirement that the source code be made available. Again, as with s 156, if the source code or other relevant data was not monitored via s 157, then any freedom of information disclosure would not assist. Like s 156, there is no requirement in s 157 that the independent monitor have suitable knowledge and technical expertise.

It is important to dwell on this last point to identify a possible ground for judicial review in the event that an unqualified auditor or monitor is appointed. Given what is now known – that electronic voting can be subverted in ways that are not obvious to someone without the requisite technical expertise who simply "observes" the process – we believe that there is a substantial argument that auditors and monitors appointed under these provisions must have those skills. It is an unsurprising principle of administrative law that, if a person makes an administrative decision in circumstances where more than lay skills are required, and the decision-maker clearly lacks the required skills to make the decision, then their decision could be made irrationally. If so, it could be susceptible to judicial review on the grounds that it is unreasonable (*Fuduche v Minister for Immigration, Local Government and Ethnic Affairs* (1993) 45 FCR 515, 527 (Burchett J)). The implications for public confidence in the electoral system are both dire and obvious.

We now come to section 158:

158 SCRUTINEERS

A candidate or registered party may appoint a scrutineer to observe:

(a) any production of the printed ballot papers and bundling and sealing of those ballot papers in accordance with the approved procedures, and

(b) any other element of the technology assisted voting process that is approved for the purposes of this section.

The breadth of s 158(b) is notable in one respect. It authorizes "a scrutineer to observe: any other element of the technology assisted voting process." This is a very wide phrase indeed and a phrase commencing with the perfectly absolute pronoun "any".

That said, the presence of the s 156 auditor and the possibility of a s 157 monitor together indicate that s 158 is describing a different process and role. Given the lengthy history of "scrutineers" it is certainly arguable that the role contemplated by this provision is the traditional one, *i.e.*, not a role requiring technical knowledge, *per se*, but just the opportunity to "observe". Observing is a less intrusive activity than auditing or even monitoring. This conclusion is reinforced by the presence of ss 156 and 157, which cannot be redundant, consistent with the principle of statutory interpretation that Parliaments do not use surplus language, and that every provision has a distinct purpose. There is a presumption in statutory interpretation that parliaments do not use surplus language, and every provision has significance (*Project*

ISSN: 1839-4183

Blue Sky Inc v Australian Broadcasting Authority (1998) 194 CLR 382 [71]).

But s 158(b) clearly elaborates on s 158(a). Does *it* have a distinctive purpose? To understand, and to also better understand ss 156-7, we need to consider these provisions in context. So we turn to s 159:

159 SECRECY RELATING TO TECHNOLOGY ASSISTED VOTING

(1) Any person who becomes aware of how an eligible elector, voting in accordance with the approved procedures, voted is not to disclose that information to any other person except in accordance with the approved procedures.

Maximum penalty: 20 penalty units or imprisonment for 6 months, or both.

(2) A person must not disclose to any other person any source code or other computer software that relates to technology assisted voting under the approved procedures, except in accordance with the approved procedures or in accordance with any arrangement entered into by the person with the Electoral Commissioner.

Section 159 contains a specific reference to "source code" but penalizes disclosure without authorization. Section 158 cannot be read in a way that makes s 159 redundant. That means that (absent such authorization) scrutiny in s 158 cannot entail access to the source code - which we argue elsewhere in this paper is necessary to enable *effective* scrutiny.

A court considering the meaning of these provisions may well have regard to the purpose of their predecessor provisions (see for example s 120AE of the *Parliamentary Electorates and Elections Act* 1912 (NSW)). Introducing the predecessor to s 156 in 2010, the NSW Government indicated that its purpose was to "guard the integrity of the system" (NSW Hansard, 24 November 2010). Reflecting on the proposed s 156, the Minister said:

> 'the bill will require an independent audit of the technology assisted voting system both before and after each general election to ensure that it properly reflects the votes cast and that it is secure. This will allow tests of the iVote system software to ensure that it is accurate and that the secrecy of votes is protected, with the system resistant to hackers and any other malicious tampering".

Our point though is that far from ensuring that audits, monitoring and scrutiny properly reflect the votes cast, s 159 mandates secrecy of the source code and thereby restricts the operation that ss 156-8 *could* have to enable proper review.

Yet, where the source code for this system remained entirely secret until months after the 2019 election, this did not reduce the exploitability of its cryptographic problems. It is by sheer good luck that Switzerland's transparency laws happened to allow the exposure of a problem with the New South Wales system. Without Swiss transparency laws, the citizens of NSW (or even the NSWEC) would have been none the wiser.

It is remarkable that there is no detailed account of this problem in the Commission's review of the 2019 election. Regrettably, source code for the iVote system remained unavailable at election time, except under a very restrictive non-disclosure agreement that prevented sharing any findings with the public for five years. (Note the deviation from the candidate-appointed scrutineering mandated for paper-based electoral processes set out below). Ultimately, four months after the election, NSWEC chose to make its source code available under reasonable terms (NSW Electoral Commission, 2019). One of us signed up for the scheme and checked the relevant part of the code, for the decryption proof problem that NSWEC had claimed was 'not relevant' to the iVote system. iVote's proof was slightly different from the equivalent part of the Swiss code, *but it was immediately apparent that the problem was still present* (Teague, 14 November 2019).

In summary, the scrutiny provisions of the NSW *Electoral Act* (ss 156-9) are weak and inadequate in protecting against the problems with the source code that we have been discussing. Specifically, the provisions:

- lack appropriate objectives by which the performance of the auditor, monitor and scrutineers can be assessed (ballot secrecy, transparency, accuracy)
- exclude effective review and analysis of the source code
- do not give that role to the independent auditor or the independent monitor

- do not require the independent auditor or monitor to have the required expertise
- do not make their work accountable, as they do not have to provide a public report about their work.
- do not guarantee that the auditor or monitor are independent, *i.e*. free from real or perceived biases, either of a political nature or in the sense of preferring to understate or hide problems.

3.3 RECOMMENDATION: THE SECRECY PROVISIONS IN NSW SHOULD BE REPLACED WITH TRANSPARENCY LAWS

Even after one of us had, with colleagues, alerted the NSWEC to the decryption-verification problem, the internal NSWEC process failed to correct it. Its continuing presence was revealed only when the source code was finally made available to independent experts months after the election.

We will argue later that sufficiently secure Internet voting under reasonable assumptions is not presently feasible in NSW. We believe that, if there is a genuinely transparent process, it will become evident that the system does not meet the crucial security requirements of elections and may well produce inaccurate results and none of us will be the wiser. We also argue that transparency about the system will help to drive better decisions about accepting its level of risk.

We will return to iVote in Section 4.3 and examine whether iVote's election data can be verified even if its cryptographic errors are corrected.

3.4 THE ACT'S EVACS SYSTEM

The Australian Capital Territory runs one of Australia's oldest e-voting systems. Voters in the ACT may vote either on traditional paper ballots or on computers in a polling place, which store an electronic-only ballot record with no paper. A separate system digitises the paper votes, combines them with the electronically-cast votes, and counts them.

From 2001 to 2016, most of the system's source code was openly available for scrutiny, which permitted valuable independent examination and identification of problems. Scientists from the Australian National University discovered errors in the code used to conduct the ACT's STV count (Goré and Slater 2020). These were found by inspecting the openly available source code and comparing it with the legislation. The most serious errors have now been corrected. In separate research, serious privacy problems were found by T Wilson-Brown, who noticed that the system retained detailed timestamps for each vote and did not shuffle votes before they were posted online, thus allowing for easy linking of individual voters with their electronic votes (Wilson-Brown 2018). We do not know whether these problems have been addressed. At the time, the Elections ACT denied the problem existed (Hayne and Bogle 2018) and since then they have not published any updates to their source code.

Two crucial gaps in scrutiny for ACT elections are in the accurate capture of voter intent, when voters cast a vote on a computer, and when a paper ballot is digitised.

The website of Elections ACT does discuss the question of whether the process for digitising paper ballots is accurate:

> *Following each election, the Commission surveys a random sample of scanned ballot paper batches from each electorate and compares the final electronic interpretation with the data included in the scanned ballot paper data file. No errors have so far been identified, indicating that electronic scanning and counting is highly accurate (ACT Elections 2020).*

This sounds comforting, until you realise that no sample size or quantification of accuracy is given, and the paper linked to as a source of 'More information' dates from 2001. Furthermore, unless such a sample is conducted transparently in the presence of scrutineers, merely reporting it does not constitute real evidence for those scrutineers. We return in Sections 5.3 and 5.4 to audits of digitisation processes – we recommend for the ACT the same process we recommend for the Senate.

The most difficult gap to fill in the ACT's system is providing voters and scrutineers with evidence that the electronic votes have been accurately recorded and conveyed through the system. When a voter presses a button on a touch screen, there is no direct evidence that the vote has been recorded as they intended – an electronic verification screen can be easily spoofed by malware, or even accidentally rendered inaccurate by configuration errors. The process of electronic transfer through the local network at the polling place, onto electronic media, and to a central counting service, also allows scrutineers no equivalent of the direct visibility of a cardboard ballot box. Again, electronic manipulation or even accidental data mishandling, could be undetectable. Voters who fill in a paper ballot, or carefully examine a paper printout, get much better evidence that the vote they intended has entered into the scrutiny process. (There is considerable controversy over whether human-readable printouts are adequate, because people often do not check them, but we sidestep that here---certainly if there is no paper at all, the voter has no opportunity to check directly how their vote has been recorded).

But a careful reading of elections ACT's website indicates an even more insidious problem:

In 2008, 2012 and 2016, an intelligent character recognition scanning system was used to capture preferences on paper ballots, with intensive manual checks used to ensure a very high level of accuracy. This data was then combined with the results of the electronic voting, and the computer program distributed preferences under the ACT's Hare-Clark electoral system. This system will again be used in 2020. [Our emphasis]

The software for the electronic voting and counting system is built in the Ada language, a coding language intended for the development of high integrity software used in systems where highly reliable operation is essential and uses open source Linux as the operating system. This combination was chosen specifically for this electoral system to ensure the election software is reliable, open and transparent, and could be made available to scrutineers, candidates and other participants in the electoral process (ACT Elections 2020).

Source code for the systems of 2001, 2004, 2008, 2012 and 2016 then follows, but it is written in C, not Ada, so it does not match the description of the 2020 system quoted above. Furthermore, ACT Electoral law was amended slightly in 2019 to change the specified algorithm for electronic counting – it must now round tallies down to 6 decimal places rather than to the nearest integer. This is unlikely to make much difference, except that it must have required an update to the code – it would not be legal to use the 2016 system again in 2020.

We requested clarification from Elections ACT and were told by email on 24 September 2020 that the 2020 code was written in Ada and, while the code could be provided "in the near future", it was not currently available because it was "currently continuing through an audit and certification process." They also added that access would require a confidentiality deed. This significant departure from their earlier policy of making it openly available was not at all evident from their website, which continued to describe the election software as "open and transparent" until several days after voting had commenced. The confidentiality deed was not attached to the email and was not available on the website but was eventually made public in response to our FoI request, two days after voting had started.

We were not the only people confused: experienced journalists described the code as "open source" in an article written at the end of the first week of polling.

Apart from the confusing statements that the code is "open and transparent" when it is in fact closed under a confidentiality deed, the deed itself defines the researcher's findings as confidential information, and has one particularly problematic provision:

5(2) "The confidant may publish its Findings only if it provides a copy of the Findings to the Territory in writing at least 60 days before the intended publication".

A period of confidentiality following security disclosures is a normal convention and is quite independent of whether the code was openly available. However, there are three reasons that this is deeply problematic in this context.

Neither the code nor the deed were available before voting started, so there was no way to inspect the code and make conclusions public in time to warn voters or explain possible errors to candidates, let alone to get errors corrected before the election.

It should also be noted that the 60-day confidentiality period overlaps the end of voting and includes the period when candidates might decide whether to accept or challenge election results. Section 259 of the *Electoral Act* 1992 (ACT) requires that a dispute about an election must be filed *within 40 days* of the declaration of the result (see also ss 256(2)(e) and 258). Elections ACT would be aware of this, of course. The 60-day confidentiality period means that it is very unlikely that the Court of Disputed Returns would be in a position to conduct "an inquiry into the accuracy of approved computer programs used in electronic voting and the electronic scrutiny of votes" (s 269(1)(b)).

In our opinion there is no reasonable justification for remaining silent after election day – if the problem is no longer exploitable, then there is a strong obligation to tell the public, to allow for an honest assessment of the accuracy of the results. There is a substantial question whether the power of the Court of Disputed Returns would be impeded by a confidentiality clause, and a legal action would likely displace it. Indeed, it is debatable whether a responsible researcher should remain silent about unpatched security vulnerabilities that only became apparent during voting: disclosure could allow voters to protect themselves from the problem by voting on paper. We accept, though, that disclosure could conceivably also increase the likelihood of exploitation by bad actors.

So while Elections ACT might superficially seem to be running a more transparent system than other Australian electoral authorities, there are important gaps in the opportunity for scrutineers to verify the process, particularly the accurate capture and electronic transfer of voter intent. We simply cannot share Elections ACT's assessment of the system as open and transparent and we regard Elections ACT's defence of it, given the confidentiality clause, disingenuous. It is not even clear that errors in the source code identified by independent researchers have been corrected. The system with openly-available source code is simply not the one that voters used.

This shows why openly available source code is valuable for error-correction, but not sufficient for election verification. Genuine scrutiny requires a way for voters and scrutineers to verify that the election has been properly conducted without trusting that the code running on the computers is the code they have been shown. In the case of EVACS, a paper record showing voters how their vote had been recorded would help, but only under the assumption that voters checked carefully for errors. The scrutiny process would then use the paper, not the electronic record. We examine methods for election verification in Sections 5 and 6.

4. SHOULD THE SOURCE CODE FOR THE SENATE COUNT BE OPEN?

We now turn to the Federal system. In 2013 Michael Cordover tried unsuccessfully to use freedom of information law to compel the AEC to publish the code it used for counting Senate votes (*Cordover and Australian Electoral Commission (Freedom of Information*) [2015] AATA 956, paragraphs [27]-[36]; see further Cordover 2014). The Senate passed a supporting motion ordering the Special Minister of State to table "the source code of the software by which Senate vote counts are conducted," but this failed to pass the House when the Minister replied, "I am advised that publication of the software could leave the voting system open to hacking or manipulation" (Sharma 2014).

This is precisely backwards: the system is highly likely to be open to hacking or manipulation, or simply bugs and configuration errors, whether or not the source code is made available. Bringing any problems out into the open is much more likely to result in them being identified and corrected.

In July 2015 Cordover's appeal to the AAT was rejected when the AEC argued that 'the documents were exempt from disclosure on the grounds that they contained information that had a commercial value that would be diminished if disclosed' (Australian Electoral Commission 2016). The 'commercial value' belonged to the AEC, who were arguing that their fee-for-service elections arm would not be able to compete effectively with commercial providers if it was forced to reveal its code (*Cordover and Australian Electoral Commission (Freedom of Information*) [2015] AATA 956, paragraphs [27]-[36]). We find it very hard to understand why the AEC's commercial incentives should trump their obligation to demonstrate that their Senate counting code is correct. We are not arguing that the AEC is disentitled to have commercial interests or concerns. Its powers and functions are broad (*Commonwealth Electoral Act* 1918, s 7). But we question the priorities reflected in its approach to Mr Cordover's application. Surely accuracy should be the number one priority of an electoral commission.

Indeed, the issue may have constitutional dimensions. Section 7 of the Australian Constitution states that the “Senate shall be composed of senators for each State, directly chosen by the people of the State”. Likewise, section 24 of the Australian Constitution states that the “House of Representatives shall be composed of members directly chosen by the people of the Commonwealth”. In their unanimous judgment in *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520 the High Court of Australia observed that these two sections are part of a suite of provisions in the Constitution that confirm that Australia has a system of *representative* government. Furthermore, the Court unanimously stated that it is *“the manner of choice of members* of the legislative assembly, rather than their characteristics or behaviour, which is generally taken to be the criterion of a representative form of government” (emphasis added) (p 559). The High Court has acknowledged that elections need to be administered having regard to “*competing considerations* relevant to the making of a free, informed, peaceful, efficient and prompt choice by the people” (*Murphy v Electoral Commissioner* (2016) 261 CLR 28 at 88 [184]; cited with approval in *Palmer v Australian Electoral Commission* [2019] HCA 14, [8]). Nevertheless, we feel confident that a requirement of *accuracy* flows directly from the constitutional mandate of *direct choice* in the constitutional provisions identified above. If we cannot feel confident that the Senate vote has not been compromised, then this not only raises cryptographic concerns, it may well raise constitutional concerns under s 7 of the Constitution. As the NSW Government noted when it introduced the predecessor provisions to ss 156-9 of the *Electoral Act* 2017 (NSW Hansard, 24 November 2010):

> *Technology assisted voting requires the operation of a complex information technology platform by, or on behalf of, the Electoral Commission as part of the crucial function of conducting elections for the New South Wales Parliament. Accordingly, the Electoral Commissioner requires a degree of flexibility in determining and approving procedures for iVoting. However, constitutional integrity of the electoral system requires that any such flexibility is limited by reference in the bill to principles of accuracy, accountability and transparency (emphasis added).*

(Unfortunately, ss 156-9 of the NSW *Electoral Act*, as we demonstrated earlier, lack the rigour and protections to enable the public to have confidence that e-voting in NSW is accurate, accountable and transparent).

We also doubt whether the code has commercial value, notwithstanding the decision of the AAT in the *Cordover* case. The notion that it has commercial value seems questionable when several free and open source alternatives exist (Silicon Econometrics Pty Ltd 2020; Bowland 2014). (We note in passing that the AAT’s decision in *Cordover* appears to have been based, at least in in part, on a concession by counsel for Cordover that the code might have commercial value: see *Cordover and Australian Electoral Commission (Freedom of Information*) [2015] AATA 956, paragraph [35]).

The practical value of using openly available source code to find errors in STV counting systems has been demonstrated in other parts of Australia. The New South Wales STV count, like the Australian Senate, uses secret code to count public data. Using that data, which includes both NSW Legislative Council and numerous NSW local government elections, Conway et al were able to compare our results with the official transcripts. This uncovered several errors in the official code, including one that (with very high probability) elected the wrong candidate to a NSW local council (Conway et al 2017). We have already described the errors in the ACT counting code, discovered by researchers at ANU. So the existence of errors in the Senate counting code is highly plausible, though no errors have ever been found.

The Senate code has become even more complex since Mr Cordover’s unsuccessful FoI application. Now there is a complex electronic process to digitise and then count the paper ballots. The public preference data allows us to double-check the counting phase, just as we can in NSW, but the rest could fail undetectably.

Based on the foregoing analysis, we recommend that legislation mandate openly-available source code for all electoral processes (readable and compilable so that a thorough examination can be conducted).

5. GENUINE AUDITING, MONITORING AND SCRUTINY OF THE DATA

In this article we have argued that *verifiability* does not come automatically in electronic systems: it is a security property that must be specifically designed into the process. In this section of the article we explore different methods for genuine auditing, monitoring and scrutiny that can help ensure verifiability. Then we demonstrate that the Senate voting system is, at present, not effectively verifiable.

5.1 "SOFTWARE INDEPENDENCE"

Although inspecting the source code can identify errors, only the election data (*i.e.* the real votes) can provide genuine evidence of an accurate election outcome. This section examines how electronic systems could be adapted to allow scrutineers to examine the votes and hence derive direct evidence of the accuracy of the outcome.

Many electronic electoral processes are not designed to permit genuine scrutiny of the data. The most notorious are the Direct-Recording-Electronic (DRE) voting machines that have been common in the USA since about the year 2000, but are gradually being phased out after a series of disastrous security and accuracy failures (Feldman, Halderman and Felten 2006; Aviv et al 2008; Checkoway et al 2009; Ottoboni and Stark 2019). DREs are used in polling places to make an all-electronic record of each person's vote. Although often characterised as a security problem, the real problem with paperless electronic voting machines is a *verifiability* problem. It is not possible to discern whether the internal electronic record correctly encodes the voter's intention or has instead been misrecorded because of a software bug, insider manipulation, or security failure.

In 2008, Rivest and Wack coined the term *Software Independent* to describe a system that provides the evidence necessary to check whether the software has correctly recorded, included and counted all the votes (Rivest and Wack 2008). A voting system is *Software Independent* if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome. The terms *Software Independent* and *verifiable* are often used interchangeably, but *verifiable* more often refers to a specific test, such as a voter's opportunity to check that their own vote is properly recorded, or an observer's opportunity to check that all votes have been correctly included in the count, whereas Software Independent describes an entire electoral process.

The most obvious way to make an electoral process software independent is not to use any software. Australia's internationally celebrated process of a manual count of hand-marked paper ballots obviously has this property. There are, however, innovative ways of engineering electoral processes to derive much of the benefit of computers, while still ensuring software independence. For example, Western Australia and South Australia have both provided computerised assistance to voters with disabilities, allowing them to use a computer in a polling place to complete a paper ballot. This is software independent because (except for voters with a severe vision impairment) the voter can directly verify that the marks on their paper ballot reflect their instructions, and then observe the paper going into a ballot box, where it enters the normal scrutiny process.

Victoria's now-discontinued vVote project used a complicated combination of voter challenges and cryptographic proofs to achieve software independence for voters in remote supervised locations such as overseas embassies (Parliament of Victoria 2017, p 162).

5.2 RISK LIMITING AUDITS

Statistical methods can also be used to verify election outcomes. Election observers can observe (or participate directly in) the audit and hence gain evidence that the election outcome is correct.

A *Risk Limiting Audit* meets a specific statistical guarantee: that if the election outcome is wrong, the audit will not pass except with some small probability (the *risk limit*) determined in advance.

Many US jurisdictions count their votes electronically but conduct a rigorous statistical audit of the paper ballots against the final count (Breedon and Bryant 2019). California Law (California Election Code § 15367) specifies mandatory post-election audits of paper ballots and includes a provision for Risk Limiting Audits. The law goes into considerable detail, defining what sort of ballot constitutes meaningful evidence of voter intent, and how the audit process should be conducted.

Note especially Section 15367(c):

"The risk-limiting audit shall be a public and observable process".

5.3 HOW COULD WE VERIFY THE SENATE SCANNING PROCESS?

Australian Senate ballots are cast on paper and then converted into electronic preferences in a complex process that combines both automated character recognition and human data entry. Unfortunately, the lack of transparency of the process means that random errors and deliberate manipulation could be possible and would not necessarily be detectable by scrutineers. It is not "software independent".

The Australian Electoral Commission claims to perform some estimates of the accuracy of its Senate scanning process, but since these are conducted away from scrutiny it is extremely difficult to find any detail about them. There is no provably risk-limiting technique for auditing the Senate count, because it is very difficult to assess whether a small change early in the elimination order has cascaded into a completely different outcome. Nevertheless, it would still be valuable to conduct a rigorous statistical audit comparing the electronic digitised preferences against the actual paper ballots. This would provide an estimate of the rate of scanning errors, could detect some forms of deliberate fraud, and, if conducted in a way that allowed *meaningful* scrutiny, provide evidence supporting the announced election outcome.

This should be conducted in a way that allows scrutineers to check both the algorithms and the data. In order to truly "observe" in the sense of gaining meaningful evidence, scrutineers would need to see the electronic digitised preferences in advance, the fair generation of random ballot selections, and the actual marks on the randomly selected paper ballots. They would then need to be (authorized to) replicate the statistical computations on their own computers if they wished.

5.4 WHO SHOULD VERIFY THE SENATE SCANNING PROCESS?

It is entirely appropriate for an authority running an information technology process to pay professionals to assess its security and reliability. Contracted code review, intrusion testing, stress testing, et cetera, are all good ways to improve the process. However, these do not perform the same function as candidate-appointed scrutineering, even if they do improve the security of the system. To put it bluntly: you have to trust the contractors, but many candidates have no reason to do so.

The Australian Parliament's Joint Standing Committee on electoral matters recommended in 2018 that the AEC appoint its own technical 'expert scrutineer' to examine the electronic Senate scanning system:

Recommendation 3 The Committee recommends that a non-partisan independent expert scrutineer be appointed to each Central Senate Scrutiny Centre in each state and territory and be responsible for:

- *auditing the computer systems and processes used to capture and count votes;*
- *undertaking randomised checks between captured data and physical ballot papers throughout the count at a level that provides surety as to the accuracy of the system; and*
- *providing reports to candidate scrutineers about their findings on a regular basis during the count (AEC 2018, p xxiii).*

When asked afterwards whether they had implemented this recommendation, the AEC replied:

... there are a number of difficulties with implementing Recommendation 3, not the least of which are

1. *The difficulties of proving 'non-partisan', 'independent' and 'expert' in relation to a scrutineer.*
2. *It is the AEC's legislated role to deliver elections in an 'independent, non-partisan' manner. Essentially, the AEC is not a participant in the election - it is the independent 'umpire'. Accordingly, the appointment of (another) independent arbitrator would create significant confusion, and potentially prevent the AEC from fulfilling its statutory function...(AEC, 6 December 2019).*

We agree. This is exactly why asking the electoral commission to select someone 'independent' and 'expert' appears *not* to have worked in NSW.

This seems to us to be an invented problem to which we already have the solution: scrutineers should be responsible for assessing whether they have been given surety as to the accuracy of the system. It is perfectly reasonable to appoint an AEC official to perform the manual work necessary to undertake randomised checks between the captured data and the physical ballot papers, *but there is no need for that person to be 'non-partisan', 'independent' or 'expert' because all their actions should be available to meaningful scrutiny by candidate-appointed scrutineers*. Hence our amended version of the JSCEM's Recommendation 3, given above. (One other pedantic point: a statistical audit can provide confidence, but not 'surety'. Certainty could be achieved only by examining all of the paper ballots).

A rigorous, statistical audit that compares physical ballot papers with electronic derived data at a level that provides confidence as to the accuracy of the result should become a normal part of the Senate vote count. Like every other part of the Senate count, it should be conducted by AEC officials and it should be designed and conducted in a way that gives scrutineers full visibility of the process so that they can verify that it has been conducted correctly.

At this point, the second part of the AEC's objection might still apply:

Further, such a process would significantly impact the efficiency of electoral processes and the timeliness of producing a result... (AEC 2019, p 12).

This is also true, but we would rather have a slowly computed correct result than a speedy one that incorporated serious error or fraud. The sky did not fall in when the 1990 Federal election result took eight days to tally (Commonwealth Parliament 1990). We feel confident that Australian democratic traditions and respect for the rule of law would tolerate delays in the production of results. Surely accuracy is a paramount consideration in an election.

The AEC concluded:

For these reasons the AEC does not intend to take any action regarding this recommendation unless legislatively compelled to do so.

We believe them. For the reasons we have developed in this article, steps should now be taken to develop and enact such legislation.

6. IS THE IVOTE PROTOCOL VERIFIABLE?

In this section we show that the NSW iVote protocol is not genuinely verifiable.

The most challenging part of an Internet voting system is what Swiss law calls *individual verifiability,* the opportunity for each voter to verify that their electronic vote accurately reflects their intention and has been properly uploaded (Guasch Castellò, no date). This step is the hardest to design because it needs to work for voters, not just technical specialists or even scrutineers. It needs to defend against system errors, insider attacks, and malware on the voter's computer, however insecure it might be. It cannot be delegated to others because the content of the vote should be private. In a polling place, the obvious solution is to ask voters to fill in a paper ballot or check a paper printout; when voting electronically from home, there is no corresponding simple check. If the method is too complex for voters to execute properly, then they may think they have verified their vote when in fact they may not have checked their vote properly.

You will recall from Section 3.1 that this was the aspect of Swiss verifiability that was shown to be unsound after already having been in use for some time. The Estonian e-voting system uses a direct cryptographic demonstration that the encryption has been properly conducted—voters have to scan a QR code and use another device to recompute and check that the correct vote has been encrypted. In some ways this is a better and more direct verification mechanism than the Swiss approach, but it is much more cumbersome and it opens up opportunities for vote selling, because voters can prove the contents of their encrypted vote.

We do not know of any secure, reliable, usable method of individual voter verification for remote e-voting in use anywhere in the world or proposed in the academic literature.

NSW votes are much more complex than votes in either Switzerland or Estonia, which further increases the difficulty of this crucial step. Swiss and Estonian voters choose one candidate or party, or sometimes one option on a referendum, while NSW voters list preferences of sometimes hundreds of candidates (Green 2019).

Unfortunately, the NSW iVote protocol does not provide a reasonable solution to this problem. The designs have varied through different rollouts in 2011, 2015 and 2019, but the most recent version asks users to download a Verification App onto a device (such as a phone) that is separate from the computer they used to vote on. Voters cast their vote using the iVote website, which then produces a QR code which the voter reads with the app on their phone. The App is then supposed to query the iVote voting server to ask (given the voter's login credentials) which vote is recorded on that voter's behalf. The App then displays the vote to the voter, who is supposed to check that it matches what they wanted.

However, both the App and the Internet voting system are provided by the same company, which gives voters no opportunity to reimplement their own 'verification app'. So we are trusting the company that provided the voting software to attest to whether its voting software accurately encoded the vote. This might be a useful check against malware on the voter's computer, but it provides no defence at all against insider attacks of the electoral commission, the software provider, or anyone who compromises them. An attacker could simply alter the vote in the voter's web browser, then use the subverted Verification App to present the voter with the vote they wanted, rather than the vote that was actually sent.

This is the central unsolved problem of remote e-voting, and it is even more complex for Australian preferential votes than it is in other countries. This motivates our recommendation to avoid paperless Internet voting altogether. We recommend that we should not allow Internet voting, email voting, web-loading PDFs or any other form of remote paperless e-voting. When votes are cast and counted manually, being able to stand in the room and watch immediately allows a scrutineer to observe that the process is running correctly. For an electronic process, the process must be deliberately and very carefully designed to provide this evidence to voters and scrutineers. If it does not provide such evidence, it is subject to undetectable fraud. There are reasonable solutions in a polling place, but verifiability remains crucial. We recommend that laws be changed to require *verifiability* for all (electronic) electoral processes.

7. THE SECRET ELECTRONIC BALLOT

There is no real electronic equivalent of a physical ballot box, which allows a voter to see that nobody else can see how they are voting. If there is malware, a key logger, or some other security problem on the computer that a person uses to cast their vote, then their vote privacy cannot be defended. Furthermore, these problems could be undetectable by the voter.

However, there are well-established cryptographic techniques for protecting the privacy of the vote after it has been cast. Since 2015, iVote has provided end-to-end encryption of the ballot between the voter's device and the electoral commission. That means that the vote is (supposed to be) encrypted in such a way such that even the electoral commission web server cannot decrypt it (but see Culnane et al 2017). Some systems (including the Swiss system) also provide a cryptographic mechanism for electronically shuffling the vote. These systems provide a guarantee of privacy that depends on electronic processes, such as the proper generation of randomness, that cannot be independently verified. Ballot privacy depends on trust.

8. COULD ELECTRONICALLY-DEPENDENT ELECTION RESULTS BE CHALLENGED?

The impossibility of verifying an electronic process relates to the difference between proving that there was a large enough problem to affect the outcome and proving that the problem worked against a specific candidate. In most jurisdictions in Australia a "court of disputed returns" has power to make orders addressing defects in voting processes." (See e.g., *Commonwealth Electoral Act* s 360(2).The *Electoral Act 1992* (ACT) allows 'that the Court may make any orders in relation to the application that the court considers appropriate' (s 265), the *Electoral Act 2017* (NSW) allows the Court to 'exercise all or any of its powers … on such grounds as the Court in its discretion thinks just and sufficient' (s 225(2)), the *Electoral Act 1992* (Qld) allows that the Court may make any order or exercise any power in relation to the application that the court considers just and equitable (s 146(1)), the *Electoral Act 1985* (SA) requires the Court to be guided by the 'good conscience and the substantial merits of each case' (s 106(1)), the *Electoral Act 2004* (Tas) requires the Court 'to be guided by the substantial merits and good conscience of the case' (s 212(2)(a)), in Victoria the Court must act fairly and according to the substantial merits of the petition' (*Electoral Act 2002* (Vic) s 126), and in WA, the relevant provision, titled 'Court must act fairly' allows that the Court can exercise all or any of its powers 'on such grounds as the Court in its discretion thinks fit and sufficient' (*Electoral Act 1907* (WA) s 126(2)). Only the *Electoral Act 2004* (NT) has no such broad enabling provision). These provisions give superior courts wide power to invalidate an election based upon any breach of the relevant *Electoral Act*. Under Commonwealth law, a court would not invalidate an election "unless the Court is satisfied that the result of the election was likely to be affected" (s 363(3)) (by an illegal practice in the instance of this particular provision). *Odgers Senate Practice* (14th ed) states:

> *Recounts normally occur only when the result of an election is very close. At any time before the declaration of the result of an election, the officer conducting the election may, at the written request of a candidate or on the officer's own decision, recount some or all of the ballot papers. The Electoral Commissioner or an Australian Electoral Officer may direct a recount.*
>
> …

There are time limits on petitions that cannot be set aside (*Rudolphy v Lightfoot* (1999) 197 CLR 500) and a Court cannot declare a *whole* general election void (*Abbotto v Australian Electoral Commission* (1997) 144 ALR 352). That said, courts have wide powers which include power to declare that any person who was returned was not duly elected; to declare any candidate duly elected who was not returned as elected; and to declare any election absolutely void. So, for example, when the AEC misplaced 1,375 ballots in the 2013 Western Australian Senate election, the WA Greens argued that reversing a difference of 14 votes, and hence eliminating a different candidate earlier in the count, would cascade into a different set of winners. They were able to produce an open-source reimplementation of the Senate counting algorithm (Bowland 2018), which allowed other interested parties to redo the count.

A challenge to iVote based on the magnitude of problems (such as the registration site crashing) might fail in NSW (because it is impossible to prove what the missing or suspect votes should have been), but succeed in a jurisdiction where it suffices to prove that the size of the problem was large enough to change the outcome. Of course, for security vulnerabilities or software errors it may be extremely difficult to assess the size of the problem, even when its existence can be clearly demonstrated. Nor is a formal challenge necessary for changing the result: Conway et al's independent implementation was sufficient to inform some candidates that their electoral loss was improbable based on the randomised count—at least one of those candidates heard about our results and demanded a recount, which, (as expected, with high probability) gave him a seat.

9. ELECTORAL COMMISSION ANALYSIS AND GUIDELINES

The electoral commissions themselves have examined the relative merits of various kinds of electronic systems, considering both their risks and their potential benefits. The AEC submitted to the Commonwealth Joint Standing Committee on Electoral Matters (2018):

> *The AEC remains of the view that the Electoral Act and related laws should be refined to remove unnecessarily prescriptive language and to further streamline processes. The language in the current Electoral Act impedes the AEC's ability to innovate and to deliver services in the most efficient manner possible.*

We think this is a false dichotomy, because well-written standards for privacy and verifiability could still allow plenty of flexibility for innovative design. Auto emissions regulations, for example, do not prevent car manufacturers from innovating, they merely prevent them from falling below an acceptable standard. They might even provide incentives to innovate to achieve further emissions reductions.

9.1 THE ECANZ ESSENTIAL PRINCIPLES

The Electoral Council of Australia and New Zealand have published eleven "essential principles for an Australian internet voting service" (NSW Electoral Commission 2019). Although not technically detailed, the intention of the guidelines seems mostly satisfactory. For example, the section on transparency is:

Transparency

The service and processes be designed to enable scrutiny, to provide stakeholder confidence.

The internet voting service and accompanying processes will be established with a focus on transparency. [...] Upon casting their vote, the service will verify to the voter that his or her intention is accurately represented and that the vote has been submitted. Any alteration to the voter's vote should be detected by the service. Voters and third parties should be able to observe the count of the votes and check that only eligible voters' votes are included in the results. The service will provide evidence that only eligible voters' votes have been included and this evidence will be auditable. Clear and unambiguous information about the internet voting service should be available to the public explaining how to use the service and how the service operates. The service should be open for verification, assurance and scrutiny purposes. Observers, to the extent permitted by law, shall be enabled to observe, comment on and scrutinise the internet voting component of an election, including the compilation of the results.

This is well-intentioned, though light on detail. Unfortunately, no Australian e-voting laws mandate any such transparency, privacy or verifiability. We have already seen that the New South Wales *Electoral Act* requires exactly the opposite. Australia's only continuing Internet voting system, the NSW iVote system, ignores this transparency principle almost entirely. As described above, the system provides very limited vote privacy, transparency only to those endorsed by the Commissioner, and no meaningful verifiability whatsoever.

For the foregoing reasons we recommend developing these principles into laws, rather than providing mere guidance. It seems highly unlikely to us that these strongly worded requirements could be met by an Internet voting system, but the principles still have value for electronically assisted voting in a polling place. For example, an electronically assisted ballot marker could help a voter with a physical disability to complete their own ballot, but still allow the person an opportunity to see their paper ballot deposited in a physical ballot box.

Our recommendations? Implement the guidelines about verifiability and transparency into law. Design an electronically assisted voting solution in a polling place for those voters who need this reasonable accommodation and ensure that it meets rigorous mandatory standards for transparency, security, privacy and verifiability.

9.2 THE WILKINS REPORT ON IVOTE

The NSWEC commissioned a report into its iVote system by Roger Wilkins AO (Wilkins 2018). It is often cited as a reason to trust in iVote's security, because its first term of reference was to assess "whether the security of the iVote system is appropriate and sufficient" (p v). However, with respect, Mr Wilkins does not have the requisite technical expertise and did not assess the code or the cryptographic protocol directly. Indeed, Mr Wilkins indicated, in the first page of his report, that "this is not a report that is going to be able to give detailed technological solutions. I do not have that expertise."

Mr Wilkins does mention the possibility of undetected fraud:

A more troubling premise might also be conceded as well. That is the contention that any system could in theory be penetrated and manipulated without the penetration and manipulation being detected (p 19).

We remain baffled by this section of the report, which seems to identify the central risk of electronic voting—the prospect of undetectable fraud—and then, like Queen Victoria's apocryphal refusal to outlaw lesbianism (Jennings 2007), argue that fraud does not need to be prevented because it could not possibly exist.

Note first that Mr Wilkins refers (throughout this section) to "penetration and manipulation" as if the first is a precondition for the second, when arguably the greatest threat (particularly for undetectable fraud) comes from insiders. Mr Wilkins then gives three reasons this threat does not need to be defended against. We pull them apart here. The first is this:

(1) As indicated in this report, I consider that on the current scale of internet voting it is unlikely that people will want to intervene to try to alter the election result. In any event, this is a matter of intelligence and it is an empirical question. The level of realistic risk is an empirical matter, and a key recommendation of this report is that electoral commissions should get very serious about integrating that intelligence into the way elections are run (Wilkins p 20).

We do not understand how the likelihood of an undetected event could be an empirical question, since by definition it cannot be tested. This is simply an assertion, without any evidence, that nobody will bother attempting fraud.

(2) In theory, while penetration and manipulation of results may not be detected, as a matter of fact it is highly likely that intervention that changed results would be detected. Psephologists, political parties, pollsters and other experts would most likely query and question outcomes that are inconsistent with expectations.

Again, respectfully, Mr Wilkins gives no specific justification of this issue of fact. We believe his assumption might be true for large manipulations, but given the recent history of very close election results at both a state and federal level in Australia, and the considerable disparities between predicted and actual poll results (Cockburn and Kontominas 2019), we do not see any adequate way of distinguishing manipulation of results from inaccuracy of predictions.

The final argument demonstrates a complete failure to understand that the key word is *undetected*.

(3) If the mere theoretical possibility of intrusion and manipulation were sufficient to stop doing things, then we would not be flying in aeroplanes, using mobile phones, and engaging in electronic commerce and banking (Wilkins p 20).

Respectfully, we wonder whether the author has ever experienced an undetected plane crash or would bank online if there was no way to tell whether money had been stolen from his account.

So this summarises perfectly the question for our electoral law: is it acceptable for electronic voting processes to permit undetectable electoral fraud, because we assume it does not exist, or is it necessary to enforce a verifiable design, so that people can verify that fraud did not occur?

If we opt for the latter, we reiterate our specific suggestions.

10. SPECIFIC RECOMMENDATIONS

We now provide a summary of the recommendations given elsewhere in this essay.

- Repeal the secrecy laws and replace them with transparency laws. The Swiss laws are a good example to follow.
- When the preference data files for Senate votes are published, there should be a rigorous statistical audit to check that they accurately reflect the paper ballots. This should be conducted in a way that allows Scrutineers to check both the algorithms and the data.
- Mandate openly-available source code for all important electoral processes. (We omit important details about exactly what "open" means for code: in this case, we would say it must be readable and compilable so that a thorough examination can be made. See the wording in the Swiss legislation, *infra*).
- Do not allow Internet voting, email voting, web-loading PDFs or any other form of remote paperless e-voting.
- Require *verifiability* for all (electronic) electoral processes.
- Develop the guidelines about verifiability and transparency into laws. Design an electronically-assisted voting solution in a polling place, for those voters who need one, and ensure that it meets rigorous mandatory standards for transparency, security, privacy and verifiability.

These recommendations are also aligned and are compatible with the AI4People recommendations on transparency and explainability for AI governance (Pagallo et al. 2019). All of the workable methods for verifying votes that we know of involve a human-readable paper record of the vote. What changes to the law would achieve all of these objectives?

11. CONCLUSION

We reiterate our observations that accuracy is of paramount importance, and indeed constitutional importance, so legislation in Australian polities that fails to enable *genuine* auditing, monitoring and scrutiny by suitably qualified professionals in order to determine accuracy should be repealed and replaced with laws that are consistent with the design principles set out above.

This will mean abandoning secrecy provisions (such as the ones in New South Wales and Western Australia) and also abandoning the current systems and processes that cannot meet minimum standards for transparency, security, privacy and verifiability. A purposive interpretation of existing electoral law would imply that candidate-appointed scrutineers are allowed an opportunity for meaningful examination of the electoral process, to the extent necessary to detect error or fraud that might change the outcome. When so many of our electoral processes are conducted by computer, a literal interpretation that allows only physical presence does not imply meaningful observation---scrutineers can look at a computer screen, but may not get evidence about what the computer is really doing with the votes.

Meaningful verifiability must be specifically designed into e-voting and e-counting systems.

Analysis of an election system and analysis of election data are complementary and both contribute positively to evidence of properly conducted electoral processes.

Openly available source code and documentation is critically important for finding errors. By carefully examining the software and its specification, observers were able were able to show critical gaps in the verification processes for both the SwissPost system and the iVote system, which allowed an attacker to produce apparently-valid proofs of an accurate election outcome that had been manipulated. Thus the opportunity to examine the code exposed a failure of verifiability.

However, examination of the code is not sufficient to give scrutineers evidence of a correct election result. Configuration errors, malware, unauthorised access or deliberate manipulation of the data might mean that the results are wrong even though no errors were detected in the code that was meant to be used. If the electoral process is not designed to produce a Software Independent evidence trail, errors or fraud could be undetectable.

Australian electoral laws should now be reformed to ensure verifiable designs, transparent software and processes, and meaningful data for candidate-appointed scrutineers to examine.

12. REFERENCES

1. Australian Capital Territory, Electronic voting and counting, https://www.elections.act.gov.au/elections_and_voting/electronic_voting_and_counting, accessed 20 August 2020.
2. Australian Electoral Commission. 2016. Managing the AEC: External scrutiny. Commonwealth of Australia <https://annualreport.aec.gov.au/2016/managing/scrutiny.html>., accessed 21 August 2020.
3. Australian Electoral Commission, Submission 120 – Supplementary Submission, Evidence to Joint Standing Committee on Electoral Matters, Commonwealth of Australia, Canberra 6 December 2019 (Electoral Commissioner (Commonwealth), Australian Electoral Commission), <https://www.aph.gov.au/DocumentStore.ashx?id=2231cf57-e040-4922-94fa-f03a06ff70d3&subId=670941>, accessed 24 August 2020.
4. Aviv, A., Černy, P., Clark, A., Cronin, E., Shah, G., Sherr, M. and Blaze, M. 2008. “Security Evaluation of Es&S Voting Machines and Election Management System.” In Proceedings of the Conference on Electronic Voting Technology, 1–13.
5. Balinski, Michel and Laraki, Rida. 2010. Majority judgment: measuring, ranking, and electing. Cambridge, Massachusetts: MIT Press.
6. Barrat i Esteve, J., Goldsmith, B., Turner, J. 2012. International Experience with E-Voting, International Foundation for Electoral Systems.
7. Bowland, G. 2018. "Counting the Western Australian Senate Election: How I ended up verifying the Australian Electoral Commission's count of the 2013 senate result" Oreamnos <https://oreamnos.com.au/posts/counting-the-wa-election/> (accessed 24 August 2020).
8. Bowland, G., Dividebatur: process single-transferable-vote elections as used for the Australian Senate under the Commonwealth Electoral Act (1918) (8 May 2014) GitHub <https://github.com/sgryphon/dividebatur>. accessed 21 August 2020.
9. Breedon, Kimberly and Bryant, Christopher A. 2019. “Counting the Votes: Electronic Voting Irregularities,

Election Integrity, and Public Corruption." The University of Memphis Law Review 49(4): 979-1017.

10. Brent, Peter. 2006. "The Australian ballot: Not the secret ballot." Australian Journal of Political Science 41(1): 39-50.
11. Brett, Judith. 2019. From Secret Ballot to Democracy Sausage: How Australia Got Compulsory Voting. Text Publishing.
12. Chancellery, Swiss Federal. 2018a. "Annex to the FCh (OEV, SR 161.116) Ordinance of 13 December 2013 on Electronic Voting - Version 2.0."
13. ———. 2018b. "Federal Chancellery Ordinance 161.116 on Electronic Voting (Veles) of 13 December 2013."
14. Checkoway, S., Feldman, A., Kantor, B., Halderman, J. A., Felten, E., Shacham, H. 2009. "Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage." Proceedings of the USENIX workshop on Electronic Voting (EVT/WOTE).
15. Cockburn, P., Kontominas, B. 2019. "Election 2019: How the polls got it so wrong in predicting a Labor victory." ABC News <https://www.abc.net.au/news/2019-05-19/federal-election-results-how-the-polls-got-it-so-wrong/11128176>, accessed 24 August 2020.
16. Commonwealth of Australia. Parliament. Joint Standing Committee on Electoral Matters. 2018. Inquiry into and Report on all Aspects of the Conduct of the 2016 Federal Election and Matters Related Thereto.
17. Commonwealth of Australia. Parliament. Joint Standing Committee on Electoral Matters. 1990. 1990 Federal Election: Report from the Joint Standing Committee on Electoral Matters.
18. Conway, A., Blom, M., Naish, L., Teague, V. 2017. "An Analysis of New South Wales Electronic Vote Counting." Proceedings of the Australasian Computer Science Week Multiconference, 1–5. <https://arxiv.org/abs/1611.02015>, accessed 21 August 2020.
19. Cordover, Michael. 2004. Software by which Senate counts are conducted, Right to Know, <https://www.righttoknow.org.au/request/software_by_which_senate_counts>, accessed 21 August 2020.
20. Culnane, C., Eldridge, M., Essex, A., Teague, V. 2017. "Trust Implications of DDoS Protection in Online Elections." International Joint Conference on Electronic Voting, 127–45. Springer.
21. Culnane, C., Ryan, P. Y. A., Schneider, S., Teague, V. 2015. "vVote: A Verifiable Voting System." ACM Transactions on Information and System Security (TISSEC) 18 (1): 1–30.
22. Federal Council of the Swiss Confederation. 2019. "Federal Chancellery to review e-voting." <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74508.html>, accessed 24 August 2020.
23. Feldman, A., Halderman, J. A., Felten, E. 2006. "Security Analysis of the Diebold Accuvote-TS Voting Machine." <https://citp.princeton.edu/our-work/voting/>, accessed 24 August 2020.
24. Ghale, M., Goré, R., Pattinson, D., Tiwari, M. 2018. "Modular Formalisation and Verification of STV Algorithms." International Joint Conference on Electronic Voting, 51–66. Springer.
25. Goré, R., Slater, A. 2003. Electronic Voting – A Review of the Hare-Clark Model of eVACS <http://users.cecs.anu.edu.au/~rpg/EVoting/evote_revacs.html>
26. Green, A. 2019. "The Battle for the Legislative Council". ABC https://www.abc.net.au/news/elections/nsw/2019/guide/legislative-council, accessed 24 August 2020
27. Guasch Castellò, S., No date. Individual Verifiability in Electronic Voting, Universitat Politècnica de Catalunya, 35-58.
28. Gumbel, Andrew. 2005. Steal This Vote: Dirty Elections and the Rotten History of Democracy in America. Nation Books.
29. Haines, T., Lewis, S. J., Pereira, O., Teague, V. 2020. "How not to prove your election outcome." 41st IEEE Symposium on Security and Privacy. <https://hdl.handle.net/2078.1/223906>, accessed August 2020.
30. Hasen, R. 2000. "Vote Buying." California Law Review, 88(5): 1323-1371.
31. Hayne, J. and Bogle, A. 2018. "Elections ACT dismisses concerns electronic ballots could be traced to voters." ABC News <https://www.abc.net.au/news/2018-08-14/voters-in-act-election-could-have-ballot-choices-identified/10115670>, accessed 21 August 2020.
32. Jennings, R. 2007. A Lesbian history of Britain: love and sex between women since 1500. Oxford: Greenwood World Publishing. Cited at <https://researchers.mq.edu.au/en/publications/a-lesbian-history-of-britain-love-and-sex-between-women-since-150>, accessed 24 August 2020.
33. Jones, D., Simons, B. 2012. Broken Ballots: Will Your Vote Count? CSLI Publications Stanford.
34. Lewis, S. J., Pereira, O., Teague, V. 2019. "Trapdoor commitments in the SwissPost e-voting shuffle proof." University of Melbourne. <https://people.eng.unimelb.edu.au/vjteague/SwissVote>, accessed 20 August 2020.
35. Lust, Aleksander. 2018. "I-Vote, Therefore I Am? Internet Voting in Switzerland and Estonia." SAIS Review of International Affairs, 38(1): 65-79.
36. Mannheim, M., Lowrey, T. 2020. "Most ACT election votes will likely be cast electronically in 2020. Here's how

electronic voting works." <https://www.abc.net.au/news/2020-10-02/electronic-voting-in-act-election-and-if-its-safe-and-secure/12722912>, accessed 5 Oct 2020.

37. Neale, R.S. 1967. "H.S. Chapman and the 'Victorian Ballot.'" Historical Studies, vol. 12, 506-521.

38. NSW Electoral Commission media unit. 12 March 2019. NSW Electoral Commission iVote and Swiss Post e-voting. <https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSW-Electoral-Commission-iVote-and-Swiss-Post-e-vo>, accessed 24 August 2020.

39. NSW Electoral Commission. 2019. "iVote Refresh for the 2019 NSW State election" <https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/iVote-Refresh.pdf>, accessed 24 August 2020.

40. NSW Electoral Commission. 2019. Report on the Conduct of the 2019 NSW State Election. <https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Election%20reports/NSW-Electoral-Commission-2019-State-election-report_Part-1.pdf>, accessed 24 August 2020.

41. NSW Hansard. 2010. Parliamentary Electorates and Elections Further Amendment Bill 2010. (Mr Aquilina.)

42. O'Collins, M. 2002. An Uneasy Relationship: Norfolk Island and the Commonwealth of Australia. ANU Press.

43. Ottoboni, K., Stark, P. B. 2019. "Election Integrity and Electronic Voting Machines in 2018 Georgia, USA." In International Joint Conference on Electronic Voting, 166–82. Springer.

44. Pagallo, U., Aurucci, P., Casanovas, P., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Schafer, B. and Valcke, P., 2019. AI4People-On Good AI Governance: 14 Priority Actions, a SMART Model of Governance, and a Regulatory Toolbox. https://www.eismd.eu/wp-content/uploads/2019/11/AI4Peoples-Report-on-Good-AI-Governance_compressed.pdf

45. PwC. 2019. Post-Election Report – Specified Procedures in relation to the online and telephone voting system ("iVote") for 2019 NSW State Election. <https://www.elections.nsw.gov.au/getmedia/b2280c43-a129-47ca-bd75-f9c98887736b/2019-State-Elections-iVote-review-(post-election-report)-June-17-2019-redactions-v2-3-draft-Copy_Redacted(1)>, accessed 24 August 2020.

46. Rivest, Ronald L. 2008. "On the Notion of 'Software Independence' in Voting Systems." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 366 (1881): 3759–67.

47. Sawer, M. 2001. "Inventing the Nation Through the Ballot Box." Papers on Parliament, No 37, November 2001.

48. Serdült, U., Germann, M., Mendez, F., Portenier, A., Wellig, C. 2015. "Fifteen Years of Internet Voting in Switzerland: History, Governance and Use." Proceedings of the Second International Conference on eDemocracy & eGovernment, 149–156. New York: Institute of Electrical and Electronics Engineers.

49. Sharma, Mahesh. 2014. "Government rejects Senate order to disclose Electoral Commission software code." Sydney Morning Herald <https://www.smh.com.au/technology/government-rejects-senate-order-to-disclose-electoral-commission-software-code-20140716-zti03.html>, accessed 21 August 2020.

50. Silicon Econometrics Pty Ltd. 2016 (last updated 21 May 2020). "Count Australian STV elections." <https://github.com/SiliconEconometrics/PublicService>, accessed 24 August 2020.

51. Teague, V. 2019. "Faking an iVote decryption proof: Why the decryption proof flaw identified in the SwissPost system affects the iVote system too." <https://thinkingcybersecurity.com/iVoteDecryptionProofCheat.pdf>, accessed 24 August 2020.

52. Tudeman, N. 1995. "The Single Transferable Vote." Journal of Economic Perspectives, 9(1): 27-38.

53. Victoria. Parliament. 2017. Inquiry into Electronic Voting. Electoral Matters Committee.

54. Wilkins, Roger. 2018. Report on the Security of the iVote System. <https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Report-on-the-Security-of-the-iVote-System.PDF>, accessed 24 August 2020.

55. Wilson-Brown, T. 2018. Possible Vote Disclosure in ACT Elections. <https://github.com/teor2345/Elections2018/blob/master/ElectionsACTDisclosure.md>, accessed 21 August 2020.

LEGISLATION

Australian legislation

Auditor-General Act 1997 (Cth), Schedule 2

Commonwealth Electoral Act 1918 (Cth), ss 7, 360, 363 and Part XVIII

Electoral Act 1992 (ACT), ss 122-3, 265

Electoral Act 2017 (NSW), Division 7, ss 156-9, 225

Electoral Act 2004 (NT), ss 46-7, 128 and Div 5 subdiv 2

Electoral Act 1992 (Qld), ss 104, 146

Electoral Act 1985 (SA), ss 67, 106 and Part 10

Electoral Act 2004 (Tas), Parts 5 and 11, and ss 172 and 212

Electoral Act 2002 (Vic), ss 76, 110, 111, 114, 116, 119 and 126

Electoral Act 1907 (WA), ss 92, 99, 117, 134, 137, 144-6.

Norfolk Island Act 1979 (Cth) (repealed)

Norfolk Island Legislation Amendment Act 2015 (Cth)

Public Finance and Audit Act 1983 (NSW), ss 27B(4) and 28

California legislation

California Election Code § 15367.

Swiss legislation

Verordnung der BK über die elektronische Stimmabgabe (VEleS) [Federal Chancellery Ordinance on Electronic Voting (VEleS)] (Switzerland) 13 December 2013 SR 161.116 articles 4.2, 5.4, 7b.

Case law

Abbotto v Australian Electoral Commission (1997) 144 ALR 352

CIC Insurance Ltd v Bankstown Football Club Ltd (1997) 187 CLR 384

Cordover and Australian Electoral Commission (Freedom of Information) [2015] AATA 956

Fuduche v Minister for Immigration, Local Government and Ethnic Affairs (1993) 45 FCR 515

Lange v Australian Broadcasting Corporation (1997) 189 CLR 520.

Murphy v Electoral Commissioner (2016) 261 CLR 28.

Palmer v Australian Electoral Commission [2019] HCA 14

Project Blue Sky Inc v Australian Broadcasting Authority (1998) 194 CLR 355

Rudolphy v Lightfoot (1999) 197 CLR 500