
The Parliament of the Commonwealth of Australia

Second interim report on the inquiry into the conduct of the 2013 federal election:

An assessment of electronic voting options

Joint Standing Committee on Electoral Matters

November 2014
Canberra

© Commonwealth of Australia 2014

ISBN 978-1-74366-243-4 (Printed version)

ISBN 978-1-74366-244-1 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.



Contents

Foreword	v
Membership of the Committee	ix
Terms of reference	xiii
List of abbreviations	xv
List of recommendations	xvii

THE REPORT

1 Introduction	1
Terms and definitions	2
Previous parliamentary comment on electronic voting	4
Conduct of this inquiry	5
2 Electronic support for the electoral process	7
Electronic certified lists	7
ECL trials	8
Benefits of ECL use	9
Expansion of ECL use	13
Committee comment	14
Online enrolment	17
Management of ballot papers	17
Committee comment	23

3	National and international experience	25
	Australian jurisdictions	25
	Federal elections.....	26
	New South Wales.....	29
	Australian Capital Territory.....	30
	International experience	31
	Brazil.....	32
	Estonia.....	34
	Ireland.....	36
	The Netherlands.....	38
	United States of America	39
	United Kingdom.....	41
	Other jurisdictions	42
	Committee comment	44
4	The use of technology in Australian elections	47
	Arguments in support of electronic voting	48
	Blind and low vision voters.....	48
	Remote voting services.....	50
	Secure handling of ballots.....	51
	Safety, cost and desirability	53
	Safety of electronic voting	53
	Cost of electronic voting systems.....	57
	Desirability of electronic voting systems.....	59
	Committee comment	65



Foreword

Our voting system has changed and evolved over the 113 years since the first federal election in March 1901. But one thing has remained a constant from the election of the first Parliament to that of the forty-fourth last September. We still vote with a pencil on a paper ballot that is then manually counted.

In recent decades some democracies have moved to a form of electronic voting. The USA has electronic voting machines in many states and Estonia offers electronic voting over the internet.

While one system requires you to still visit a polling booth and the other offers online convenience, advocates argue that both offer faster and potentially more accurate results.

With the close of polls the results are known within minutes rather than hours, days and weeks and arguably without the human error that occurs in the long paper ballot count.

Many think it sounds like a good idea for the next federal election.

No matter your view, this is not feasible.

Even the most ardent electronic voting advocates must recognise that in logistical terms it would be impossible for our electoral authorities to roll it out next polling day which is less than two years away – at the latest.

But what about future elections?

I once simply assumed so, but that was before I had really given it a lot of thought.

After hearing from a range of experts, and surveying the international electoral landscapes it is clear to me that Australia is not in a position to introduce any large-scale system of electronic voting in the near future without catastrophically compromising our electoral integrity.

Machine electronic voting at a polling place is vulnerable to hacking to some degree. This can be mitigated by a system that not only records your vote electronically, but also produces a printed ballot for physical counting and later

verification. In other words, a lot of expense to still visit the polling booth, queue up and complete your vote on a machine rather than a paper ballot.

For this reason, internet voting seems to be naturally the most attractive to many voters. As an election expert from the USA recently said to me: 'when it comes to voting, folks would rather be online than in line.'

But the weight of evidence tells us that at present this is highly vulnerable to hacking.

While internet voting occurs in Estonia, it does not mean that system cannot be hacked. With all the internet security architecture available, the academic experts swear they can, and have proved they can, hack such systems.

In future it is likely, given the turbo-advances in technology, that a system of online electronic voting could be delivered with acceptable safety and security. But even when we reach that time, there should be considerations beyond the convenience it would offer.

Given we complete so many transactions online, I am often asked why voting should be any different. My answer to that is that voting once every three years to determine our democratic destiny is not an everyday transaction.

Not only do we have the right to a ballot; we have rightly enshrined within our system the right to a secret vote. Voting at a booth in a polling place guarantees this; voting over the internet threatens this.

Internet voting would expose some voters to family and peer pressure by removing the individual isolation of voting at a secluded booth and replacing it with voting in a home, a workplace or a public place. It also potentially opens up a market for votes where disengaged or financially desperate voters could be offered money to vote a certain way, which could be verified in a way not possible at a polling place.

This is not to say that we should not be striving to make better use of modern technology, but it is to say that technological convenience must be balanced against electoral integrity.

There are other aspects of our voting process that should be brought into the modern electronic world; aspects that will not compromise the security, sanctity and secrecy of the ballot.

We can progressively replace the paper roll at each polling booth with an electronic interconnected roll. At present every booth within an electorate has an identical paper roll. When you vote your name is crossed off at the polling place you attend. With an interconnected electronic roll, when your name is crossed off and you are provided with a ballot, it will be almost simultaneously crossed off at every other booth. That will reduce the opportunity for multiple voting in your name at other polling places and will reduce administrative errors.

At the same time we should start to introduce electronic scanning of ballot papers. This enables an electronic count, the results of which would be delivered minutes after the close of the polls. The same physical count that occurs now would still be performed for verification.

Such a system would offer faster results, at a manageable cost without any of the risks or compromises of electoral integrity of stand-alone electronic voting. Indeed, it would provide a checking mechanism, providing a measure of surety to the count.

This report makes seven recommendations to this end. Recommendations 1 to 4 call for the roll out of electronic certified lists to all pre-poll centres and mobile voting teams initially, with the eventual introduction to all polling places. The Committee also considers that there is opportunity for this technology to be developed collaboratively and shared with the states and territories.

Recommendations 5 and 6 propose the consideration of electronic counting and storage of ballot papers. This would offer a number of benefits in terms of speed and verification of the count. Should ballots be scanned for counting, they may also be able to be stored digitally. Currently ballot papers are destroyed after a prescribed number of years. If scanned and stored digitally, they could be retained indefinitely and in doing so, capture part of the electoral history of Australia.

Finally, the Committee acknowledges the real benefit of the current telephone assisted voting system that is available to blind and low vision voters and recommends that it be extended to voters with assessed mobility or access issues to provide them with easier access to voting.

I want to place on the record my thanks to the members of the Committee, the Hon Alan Griffin MP, Senator Matthew Canavan, Senator the Hon John Faulkner, Ian Goodenough MP, Hon Gary Gray MP, Senator Chris Ketter, Senator James McGrath, Tony Pasin MP and Senator Lee Rhiannon. Senator Chris Back has also shown great interest in this issue as a participating member.

The Committee has already completed an extensive series of hearings in relation to this inquiry and this is the second interim report issued. Over the course of the twenty hearings to date and in reviewing the 207 submissions received, the Committee has worked collaboratively and in an impartial manner to ensure that the best outcomes have been met.

Technology is moving at a rapid pace. The Committee believes that we should be utilising it to ensure that the systems underpinning how we vote are sound and that persons with disabilities have easy access to the vote. In doing so, we will harness that which enhances our electoral integrity, not that which endangers it.

Hon Tony Smith MP
Chair



Membership of the Committee

Chair Hon Tony Smith MP

Deputy Chair Hon Alan Griffin MP

Members Ian Goodenough MP

Gary Gray MP

Alex Hawke MP (to 14 July 2014)

Tony Pasin MP (from 14 July 2014)

Senator Matthew Canavan (from 1 July 2014)

Senator the Hon John Faulkner

Senator Chris Ketter (from 1 July 2014)

Senator Helen Kroger (to 30 June 2014)

Senator James McGrath (from 1 July 2014)

Senator Lee Rhiannon

Senator Anne Ruston (to 30 June 2014)

Senator Memhet Tillem (to 30 June 2014)

Participating members for the purposes of the inquiry into the 2013 federal election (as at 18 November 2014)

Senator Chris Back

Senator Cory Bernardi

Senator Catryna Bilyk

Senator Carol Brown

Senator Joe Bullock

Senator David Bushby

Senator the Hon Doug Cameron

Senator the Hon Kim Carr

Senator the Hon Jacinta Collins

Senator the Hon Stephen Conroy
Senator Sam Dastyari
Senator Sean Edwards
Senator David Fawcett
Senator Alex Gallacher
Senator the Hon Bill Heffernan
Senator David Leyonhjelm
Senator Sue Lines
Senator the Hon Joe Ludwig
Senator the Hon Kate Lundy
Senator the Hon Ian Macdonald
Senator John Madigan
Senator John Madigan
Senator Gavin Marshall
Senator Anne McEwen
Senator Bridget McKenzie
Senator the Hon Jan McLucas
Senator Claire Moore
Senator Ricky Muir
Senator Deborah O'Neill
Senator Barry O'Sullivan
Senator Nova Peris
Senator Helen Polley
Senator Linda Reynolds
Senator Anne Ruston
Senator Zed Seselja
Senator Lisa Singh
Senator Dean Smith
Senator Glenn Sterle
Senator Anne Urquhart
Senator John Williams
Senator the Hon Penny Wong
Senator Nick Xenophon

Committee Secretariat

Secretary	Dr Nicholas Horne (from 7 August 2014) Dr Glenn Worthington (to 3 July 2014)
Inquiry Secretary	Siobhán Leyne
Technical advisor	Jeff Norris
Administrative Officer	Jessica Ristevska



Terms of reference

On 5 December 2013, the Special Minister of State, Senator the Hon Michael Ronaldson, requested the Committee to conduct an inquiry with the following terms of reference:

That the Joint Standing Committee on Electoral Matters inquire into and report on all aspects of the conduct of the 2013 federal election and matters related thereto.



List of abbreviations

AEC	Australian Electoral Commission
ADF	Australian Defence Force
ECANZ	Electoral Council of Australia and New Zealand
ECL	Electronic certified list
EVM	Electronic voting machine
IDEA	Institute for Democracy and Electoral Assistance
NSWEC	New South Wales Electoral Commission
TSE	Tribunal Superior Eleitoral (Brazil)



List of recommendations

2 Electronic support for the electoral process

Recommendation 1

The Committee recommends that the Australian Government adequately resource the Australian Electoral Commission to deploy electronic certified lists where possible to all pre-poll voting centres and to all mobile voting teams at the next federal election.

Recommendation 2

The Committee recommends that, after the next federal election, the Australian Electoral Commission undertake a full cost benefit analysis of utilising electronic certified lists at all polling locations based on a permanent investment in the relevant technology and/or the development of a platform that can be accessed from any networked computer, with a view to full implementation at future elections.

Recommendation 3

The Committee recommends that the Special Minister of State propose to the states and territories that the further development of electronic electoral roll mark-off systems be undertaken in a collaborative approach to facilitate the sharing of resources.

Recommendation 4

The Committee recommends that relevant sections of the *Commonwealth Electoral Act 1918* and the *Referendum (Machinery Provisions) Act 1984*, be amended to allow for the expansion of the use of electronic certified lists as a form of approved list for marking electors who have been issued a ballot paper.

Recommendation 5

The Committee recommends the Australian Electoral Commission develop and trial the electronically-assisted counting of ballot papers at all pre-poll centres for the next federal election.

Recommendation 6

The Committee recommends that the Australian Government investigate the feasibility of digital storage of scanned ballot papers to replace storage of paper ballots.

4 The use of technology in Australian elections

Recommendation 7

The Committee recommends that the *Commonwealth Electoral Act 1918* and the *Referendum (Machinery Provisions) Act 1984* be amended to allow for expansion of the current assisted telephone voting system to include people with assessed mobility or access issues for the next federal election.

Introduction

- 1.1 Following the loss of ballot papers during the 2013 federal election, there has been significant public discourse about potential technological improvements to our electoral system that would reduce the likelihood of a repeat of such events and other systems problems from occurring.
- 1.2 There can be little disagreement with the idea that the electoral system needs to harness the technology available to it, and there are many aspects of the electoral system where these reforms can be introduced, including building capability in electronic support for voting.
- 1.3 Chapter 2 of this report argues that the best first steps towards modernising the electoral system in this context should be through electronic support systems – expansion of electronic certified lists (an electronic roll); digital count of ballot papers; and digital storage of ballot papers, online advice and support to inform electors of voting and to provide online support for electors with a disability.
- 1.4 These are all mechanisms that will enhance and improve the electoral system. They have an inbuilt layer of scrutiny, maintain the sanctity of the ballot, enhance electoral integrity and, critically, can begin to be readily implemented at the next election.
- 1.5 In the wake of the lost ballot papers fiasco at the 2013 Western Australia Senate election, there have naturally been calls for a move beyond this to electronic voting. One argument here is that, as the Australian public is comfortable with digital technology, a move to electronic voting should be straightforward:

The Saturday Age suggests the controversy surrounding the AEC provides an opportunity to improve Australia's democracy. We believe the Government should commission an expert inquiry with a view to introducing electronic voting, preferably in time for

the next federal election. After all, digital technology has revolutionised so much, and people have become comfortable and confident banking, shopping and storing private information online. A secure system operating only within authorised facilities would be a relatively straightforward exercise.¹

- 1.6 This report undertakes an extensive consideration of electronic voting. Chapter 3 surveys the experience of national and international jurisdictions with electronic voting. This analysis makes it clear that, rather than Australia being left behind by not having widespread electronic voting in place, many jurisdictions are abandoning the decades of significant investment in this technology due to high maintenance costs, as well as secrecy and security concerns.
- 1.7 Chapter 4 assesses proposals to implement electronic voting in Australia. This assessment identifies significant questions over the capacity of an electronic voting solution to be both cost-effective and protect the security and sanctity of the ballot in the Australian context.
- 1.8 The report concludes, irrespective of one's philosophical view about electronic voting, that there can be no widespread introduction of electronic voting in the near term without massive costs and unacceptable security risks.
- 1.9 Any use of technology in association with the electoral process must have the principle of the sanctity of the ballot at its core, including upholding the right to a secret ballot and ensuring transparency in the counting process.
- 1.10 The Committee acknowledges that, following the events of the 2013 federal election, the Australian Electoral Commission (AEC) is undergoing a period of significant organisational reform and re-evaluation of standard operating procedures that will improve its delivery of the electoral system. The recommendations in this report will enhance the AEC's efforts to improve its service delivery.

Terms and definitions

- 1.11 The term 'electronic voting' broadly describes a variety of practices and technologies that can facilitate voting, recording and counting. The term extends to systems in which the act of voting occurs with the assistance of electronic technology; where votes are recorded, captured or stored electronically; and where votes are loaded into a computerised counting system to determine election results.

1 *Saturday Age* editorial, quoted in Democratic Audit of Australia, *Submission 116*, p. 5.

- 1.12 In this report, ‘electronic voting’ is used to refer to technology associated with the act of voting, and ‘electronic support for voting’ is used to refer to electronic mechanisms which support the electoral process more generally.
- 1.13 Electronic support for voting includes:
- **Electronic certified lists** – where a computerised electoral roll is produced for use in polling places or with mobile voting teams. This electronic support solution allows for more accurate and real-time mark-off of voters from certified lists, as well as faster processing of declaration votes.
 - **Electronic counting and scanning** – systems can be developed that allow for either manual electronic entry of ballot papers (such as is currently done for below-the-line Senate votes) or automated scanning of ballot papers where vote data is entered via intelligent software recognition (such as is used in the Australian Capital Territory).
 - **Online enrolment and update** – where a voter can enrol for the first time online, or go online and update their enrolment details. This is especially advantageous during the close of rolls period at the start of an election, as immediate updating of details significantly lessens the administration of updating systems from paper forms.
- 1.14 The act of electronic voting encompasses all of the following:
- **Electronically-assisted voting** – allows blind or low vision voters to complete a ballot paper with the assistance of an operator or audio prompts delivered via the telephone or through an electronic voting machine. Such electronically-assisted voting was trialled in the 2007 federal election and has been a feature of recent federal elections as well as elections in three states and territories in recent years.
 - **Isolated static electronic voting** – involves using computers or custom-built electronic voting machines which are configured as stand-alone devices or are connected together on an isolated local area network but which are not linked to the broader internet. This form of remote electronic voting was trialled by the AEC in conjunction with the Australian Defence Force (ADF) in 2007. In this trial, ADF personnel on overseas deployments were able to access a secure computer network that enabled them to cast their vote.

- **Internet voting** – this can be split into various categories:
 - ⇒ *static internet voting* – requires the voter to be present in a polling location, using a dedicated computer or network to access the relevant internet page to cast their vote. This model is most similar to the current form of voting in that it allows the electoral authority to maintain control over the hardware or network used to vote and the environments in which votes are cast.
 - ⇒ *mobile internet voting* – where, for example, the electoral authority organises mobile polling teams to visit voters in their homes or certain localities with portable devices connected to the internet which voters then use to vote. This allows the electoral authority to maintain control over voting hardware and the circumstances in which a voter exercises their franchise, while utilising the portability of electronic technologies to maximise voting accessibility.
 - ⇒ *remote internet voting* – the most expansive model of internet voting and what is most commonly meant by the term ‘internet voting’. Remote internet voting allows the voter to cast their vote from any device with internet access. In this situation there are significant difficulties with verifying voter identity, or whether a voter may be casting their vote in secret and free of coercion. The electoral authority also has very little control over the hardware and associated software used by the voter and almost no control over the environment in which voting occurs.

Previous parliamentary comment on electronic voting

- 1.15 Previous Electoral Matters committees have considered the issue of electronic voting at some length, both in reviews of specific elections and independent inquiries. This Committee, along with its predecessors, have approached this issue with a view to balancing the enfranchisement of the electorate with the security and cost-effectiveness of the ballot. As such, previous inquiries have consistently found that while there are benefits to electronic voting, these benefits do not outweigh security concerns and the cost.²
- 1.16 In its report on the 2004 federal election, the Electoral Matters Committee of the 41st Parliament the Committee stated:
-

2 Joint Standing Committee on Electoral Matters, June 2003, *Report of the Inquiry into the conduct of the 2001 federal election, and matters related thereto*, Canberra, pp. 267-268; Joint Standing Committee on Electoral Matters, September 2005, *Report of the Inquiry into the conduct of the 2004 federal election and matters related thereto*, Canberra, pp. 257-258.

attendance at a polling place [is] a key contributor to Australia's democracy. If all Australians were given the opportunity to vote remotely, the Committee believes one of the best features of Australia's voting system would be removed. Therefore, even if it is technologically possible, the Committee has no desire to see widespread remote electronic voting introduced at any time in the future.³

- 1.17 In the Electoral Matters Committee of the 42nd Parliament in its 2009 report on the 2007 election electronic voting trials for blind and low vision voters and remote Defence personnel, the Committee found that the cost was unsustainable and that the administrative obligations on Defence personnel were significant and unreasonable. The Committee recommended that the trials be discontinued.⁴
- 1.18 Notwithstanding these reports, there has been some parliamentary support for the implementation of electronic voting. In 2013, the House of Representatives Standing Committee on Regional Australia tabled its report on the use of 'fly-in, fly-out' workforce practices in regional Australia. In examining the enfranchisement of remote workers, the Committee recommended that electronic voting be implemented, stating that 'electronic voting may be the most accessible method of providing access to these workers to vote.'⁵

Conduct of this inquiry

- 1.19 The Committee has examined electronic support for voting and the merits of electronic voting in the context of its wider inquiry into the conduct of the 2013 federal election, referred by the Special Minister of State on 5 December 2013. As part of that referral, the Minister requested the inquiry specifically analyse the issue of electronic voting.
- 1.20 Given the commentary on the issue of electronic voting in the media, amongst participants in the inquiry, and more generally in the national and international electoral context, the Committee decided to produce an interim report on electronic voting and electronic support for voting. This

3 Joint Standing Committee on Electoral Matters, September 2005, *Report of the Inquiry into the conduct of the 2004 federal election and matters related thereto*, Canberra, p. 271.

4 Joint Standing Committee on Electoral Matters, March 2009, *Report on the 2007 federal election electronic voting trials*, Canberra.

5 Standing Committee on Regional Australia, February 2013, *Cancer of the bush or salvation for our cities? Fly-in, fly-out workforce practices in regional Australia*, Canberra, p. 129.

early response will also enable the Australian Government to respond to the Committee's recommendations well before the next federal election.

- 1.21 The Committee has conducted public hearings and private briefings on this issue as part of the hearing and meeting programme undertaken for the overarching 2013 federal election inquiry. All transcripts and submissions are available on the Committee's website⁶ and a full listing will be included in the final report.

6 <aph.gov.au/em>.

Electronic support for the electoral process

- 2.1 There are many aspects of the electoral system that can be enhanced with better utilisation of electronic technology. Not only can these changes improve the voter experience, critically, they can also enhance security and therefore build further confidence in our electoral system.
- 2.2 The Australian Electoral Commission (AEC) already makes use of online enrolment, and trials of electronic certified lists, to replace the traditional paper electoral roll in polling places, were successfully undertaken during the 2013 election, the 2014 Griffith by-election and the 2014 Western Australia (WA) Senate election. There is also potential for the use of existing scanning and character recognition software to support the counting and storage of ballot papers.

Electronic certified lists

- 2.3 Federal certified lists are the compiled electoral rolls for each division, completed after the close of rolls period (currently seven days after the issue of the writs for a federal election). The lists are an essential part of election day and are used to manually mark-off a voter as having attended a polling place and having been issued a ballot paper.
- 2.4 Certified list data is used in AEC systems to conduct:
 - 'preliminary scrutiny' of a declaration voter's eligibility to vote and admission of their vote to the count; and
 - post-election day comparison of the electoral roll and marked certified list data to identify non-voters or individuals having voted multiple times.

- 2.5 These lists are custom-printed for each division, then distributed to every relevant static polling place, pre-poll centre and mobile voting team in the country. The manual mark-off of these paper lists has become a familiar part of the process of voting in Australia.
- 2.6 The AEC commenced a pilot trial of electronic certified lists (ECLs) at the 2013 election, as well as at the following Griffith by-election and 2014 WA Senate election. These trials also resulted from recommendations of the previous Electoral Matters Committee in relation to the conduct of the 2010 federal election.

ECL trials

- 2.7 For the trials, the ECL involved a custom-made software platform consisting of an electronic copy of the certified list on a laptop used in polling booths in place of the paper list:
- ECL devices used a mobile broadband network which allowed the AEC to more efficiently and accurately search for and mark names off the electoral roll, reducing electors' queuing times, among other benefits. Certified list data was loaded onto laptops and a range of features were trialled in various polling situations to determine how the technology could best be used on a wider scale. ECLs provide the ability to search for and mark an elector's name off the certified list, provide real-time update to a central copy of the certified list when network connectivity is available, print House of Representative ballot papers on-demand and record that a declaration vote has been issued.¹
- 2.8 For the 2013 federal election, a total of 768 ECL devices were deployed to different locations across Australia to be used for both vote issuing and preliminary scrutiny. Following the 2013 election pilot project the AEC concluded that:
- During the pilot, a sample of electors was surveyed to assist the AEC in identifying both the success of the ECLs and electors' confidence in the voting process. Eight polling places using ECLs were included in the research; seven on election day and one during pre-polling. The survey results showed that ECLs tended to improve voter satisfaction in terms of how easy and quick it was to find and mark electors' names off the list. Those casting a vote at an ECL location were much more likely to be 'very satisfied' with the length of time taken to vote than at non-ECL locations; 83 per cent in ECL locations, compared with 56 per cent.

1 Australian Electoral Commission (AEC), *Submission 20.3*, p. 71.

However, pre-poll voters surveyed were less confident that their personal information and privacy was kept safe and secure in ECL locations than those in non-ECL locations; only 66 per cent reported that they were very confident in this instance where there were ECLs, compared to 82 per cent in non-ECL locations.²

2.9 ECLs were also used at the Griffith by-election and WA Senate election. In respect of these trials the AEC reported that:

At the 2014 Griffith by-election, 145 ECLs were then used at all ordinary issuing points and 230 ECLs were also used at the 2014 WA Senate election for all remote mobile polling, the majority of pre-poll voting and at the Perth Superbooth on polling day at ordinary and declaration issuing points.³

2.10 There have also been calls for ECLs to be utilised in elections as a method of combating multiple voting. The pilot projects have been successful in reducing the incidence of multiple marking off of lists.

2.11 A number of benefits of the ECL platform have been identified including:

- improvements in marking of certified lists and fewer associated errors;
- reduction in the need to transport and scan paper lists;
- alignment with contemporary systems at state and international levels;
- electronic monitoring of pre-poll and mobile polling activity;
- ease of transport for mobile teams; and
- improved accuracy and speed in processing and counting declaration votes.⁴

2.12 These are considered further below.

Benefits of ECL use

2.13 There are two primary benefits to the use of ECLs:

- lower marking error rates made by polling officials; and
- lessen the opportunity for deliberate multiple voting through:
 - ⇒ identifying those attempting to vote multiple times as they attend a second and subsequent polling booth; and
 - ⇒ identifying those trying to vote in another person's name.

2 AEC, *Submission 20.3*, pp. 72-73.

3 AEC, *Submission 20.6*, p. 32.

4 AEC, *Submission 20.3*, pp. 33-34.

- 2.14 During the 2013 federal election, 18 770 multiple marks (persons marked off the electoral roll more than once) were identified. The AEC wrote to all electors identified and of these multiple marks:
- 10 671 were attributable to polling official error;
 - 2 013 electors admitted to multiple voting;
 - 6 000 have still not responded or responded inadequately and remain unresolved.⁵
- 2.15 The issue of multiple voting will be addressed in the Committee's final report. However, the use of ECLs offers the potential to identify these instances as they occur.
- 2.16 The other benefits to the use of ECLs are:
- reduction in the use, and cost, of paper list production;
 - alignment with other Australian jurisdictions and collaboration potential; and
 - improving the speed and accuracy of counting and scrutiny of the admissibility of declaration votes – which will again identify potential multiple voters at a stage before votes are admitted to the count.

Lower error rates associated with certified list marking

- 2.17 A significant number of apparent roll mark-offs that would seem to indicate multiple voting incidents is attributable to official error (an issuing officer marking a certified list incorrectly). The use of ECLs would offer a significant reduction in the official error rate.
- 2.18 The 2014 Griffith by-election offered an opportunity to test for the impact that exclusively using ECLs can have on the error rates for vote issuing and potential multiple voting, as well as any other associated benefits or problems.
- 2.19 The AEC reported that, for the division of Griffith, the incidence of multiple marks on certified lists between the 2013 election and the by-election reduced by 75 per cent – down from 180 for the 2013 election to 44 for the by-election.⁶ This reduction in multiple marks is an improvement over the usual results for a federal division in an election where an identical paper roll is used in every polling place.

5 Senate Finance and Public Administration Legislation Committee, *Additional Estimates 2013-2014, Answers to Questions on Notice, Question F69*, 11 April 2014. Marie Neilson, Assistant Commissioner, Elections, AEC, *Transcript of Evidence* from Senate Finance and Public Administration Committee, 29 May 2014, Canberra, p. 116.

6 Marie Neilson, Assistant Commissioner, Elections, AEC, *Transcript of Evidence*, 31 July 2014, Canberra, p. 14.

- 2.20 The effort, time and resource savings from reduced numbers of multiple marks should be substantial, especially with the multifaceted response required by the Electoral Act in investigating marks, writing to voters, compiling evidence, and actioning referrals of multiple voters to the Australian Federal Police. These follow-up actions constitute a substantial commitment of time and effort by the AEC and delay the finalisation of election work.
- 2.21 There is an additional associated benefit stemming from ECL use in that a lower incidence of incorrect mark-off should result in lower associated numbers of incorrectly identified non-voters. More accurate search and mark-off of voters from ECL devices means that the incidence of the same person being marked off two paper certified lists in error is lowered, potentially also lowering the incorrect identification of the voter as a non-voter.
- 2.22 Currently the AEC investigates both potential non-voters and multiple marks after each election. Reduced incidence of incorrect mark-off resulting from ECL use should lead to fewer non-voter investigations, resulting in significant time and resource savings in that area of post-election activity.

Less opportunity for deliberate multiple voting

- 2.23 For any person who wishes to deliberately break the law by voting multiple times, it is relatively easy for that person to attend multiple polling places and assert that they have not voted elsewhere. It is only when the paper lists from for the division are compared after the election that such examples of apparent multiple voting can be identified.
- 2.24 The universal use of ECLs would go some way to eliminating this problem. On the first occasion that a person attended a polling booth, their name would be marked off the list and this would be automatically marked off in the electronic roll central database which would then be reflected in every polling place.⁷
- 2.25 Should that person or someone else seeking to vote in their name then attend another polling booth, they would be unable to cast an ordinary ballot and would be referred to cast a declaration vote. This could then be prevented from being admitted to the count upon verification that they had already voted, and would at least identify a problem at the second instance - whereas with a paper-based roll there are theoretically as many multiple voting opportunities as there are polling places within a division.

7 This is reliant on the ECL having a network connection.

Paper list reduction

- 2.26 While there was no reduction in the supply of paper certified lists during the recent election trials due to the need for a backup in case of ECL failure, longer-term reductions in the supply of paper lists should result over time from wider ECL use.
- 2.27 The current requirement to scan the paper lists after every election in order to electronically capture the data that identifies correct marks, non-voters, or multiple marks, also adds a further logistical dimension to paper certified list usage, as well as additional cost, as third-party contractors must be engaged to undertake the scanning and data capture process.
- 2.28 The requirement to physically transport certified lists across the country and with mobile voting teams would be eased with the usage of ECLs. The other added advantage of ECL usage here is that one device can hold certified list data for all divisions; this would lessen the requirement for teams to take multiple lists if transitioning between divisions or taking interstate votes, enabling the AEC to better direct and allocate its resources.
- 2.29 ECLs were capable of producing an emergency stock of ballot papers, or stock of other division ballot papers, during the 2013 election. If this functionality was continued, transport burdens would be reduced even further. Ballot paper security, custody and verification must remain a key priority; but there is potential for real benefit and cost savings.
- 2.30 The use of ECLs has the added functionality of digitising the capture of polling activity (number of votes issued, time taken for queues to progress) as well as monitoring productivity and digitising the recording of activity at certain times of the day. The recording of this data has been manual in the past, with Officers-in-Charge of polling places recording work levels and votes issued; there has also been a requirement for those records to be communicated to the Divisional Returning Officer and entered into the relevant election IT systems. Reducing the administration associated with this work would leave Officers-in-Charge more time to manage other important polling day activities such as the safe storage and handling of ballot papers.

Alignment with other jurisdictions and collaboration potential

- 2.31 Electronic support systems similar to ECLs, for marking voters off certified lists, already exist in other states and territories. All states and territories have trialled or are using some form of electronic roll look-up or mark-off system, for either state or local government elections – for instance the ACT has used electronic mark-off during elections since 2008

- (both on PDAs and laptops) and NSW has had an evolving system since 2007 (starting with look-up only, to mark off systems).
- 2.32 Some state/territory electoral commissions are also actively monitoring the outcome of the ECL trial for the federal election prior to investing in similar systems.⁸
- 2.33 This usage of electronic roll mark-off systems at the council and state level builds awareness of technological improvements in voting systems. Voter familiarisation with these types of systems could smooth the transition to wider ECL usage federally, as could the presence of polling officials familiar with electronically-aided vote issuing.
- 2.34 There has been limited sharing of resources in this space in the past, with the AEC sharing roll personal digital assistant architecture with state electoral commissions. Shared development and a commitment to enhancing electoral roll integrity and harmonisation can be further supported by a collaborative approach to expansion of ECL systems and architecture.

Counting and scrutiny benefits

- 2.35 ECLs can be used for preliminary scrutiny of declaration vote envelopes (where a voter's eligibility to have their vote admitted is tested) and were used extensively at the 2013 election, the Griffith by-election and the 2014 WA Senate election.
- 2.36 The preliminary scrutiny of the declaration votes process requires intensive scrutiny of enrolment eligibility. Electronic support for this process through ECLs proved very useful for the speed of processing and for the accuracy and consistency of decisions on whether to admit a declaration vote or not.

Expansion of ECL use

- 2.37 Given the trial nature of ECL development and deployment up until now, the AEC developed the ECL application software itself, but the hardware was leased and logistics support was provided by third parties. This resulted in a \$1 400 per unit cost, which would be unsustainable into the future if any expansion was considered.
- 2.38 The AEC has expressed the view that, with further resourcing and development, the ECL function is scalable; however, without further

8 Northern Territory Electoral Commission, *Annual Report 2012-2013*, p. 23.

development, costs and implementation impacts can only be calculated based on the trials.⁹

- 2.39 The AEC provided detailed information on the barriers to, and costs of, universal expansion of the use of ECLs in the future. In summary, a wholesale roll-out of ECLs in their current software and hardware configurations would be prohibitively expensive, with indicative costs of over \$65 million for deployment to all 150 divisions.¹⁰
- 2.40 With an overall cost for the 2013 federal election of approximately \$191 million, an increase in costs of that magnitude in regard to certified lists alone is not justifiable.¹¹
- 2.41 The AEC has indicated that a full deployment of ECLs to all mobile voting teams, which benefit greatly from the reduced inventory an ECL creates, and to all pre-poll voting centres for the next federal election, would be an appropriate next step in development and would cost approximately \$12.8 million based on the current platform.¹²

Committee comment

- 2.42 ECLs offer significant benefits for the delivery of election support services through an improvement in the timeliness and accuracy of roll mark-off management, reduction in paper lists, alignment with other jurisdictions, improvement in the management of declaration votes, and a reduction in the work associated with post-election activities such as scrutinising lists for multiple votes or non-voters.
- 2.43 The Committee is of the view that ECLs are an important step forward in improving election delivery in Australia and are worthy of significant investment by the Australian Government. The very positive response from surveyed voters participating in the 2013 election ECL trial in respect of satisfaction with reduced voting time is significant.
- 2.44 At the same time, the doubts expressed by one-third of the surveyed ECL trial pre-poll voters regarding the security of their personal information and privacy in ECL locations are salutary, and point to the crucial importance of ensuring security and integrity of voter information as well as the wisdom of caution in relation to electronic voting beyond electronic support.
- 2.45 Targeted further development of ECLs should allow the AEC to invest in improving the ECL platform and also concentrate on making the platform
-

9 AEC, *Submission 20.6*, p. 32.

10 AEC, *Submission 20.6*, p. 38.

11 AEC, *Submission 20.3*, p. 133.

12 AEC, *Submission 20.6*, p. 38.

more robust when mobile, and potentially deliverable across multiple types of devices (the current ECL platform requires a standard laptop). The development of this further platform could also potentially inform growth and development in other Australian jurisdictions.

- 2.46 As the use of ECLs becomes more widespread, there should be the capacity for the AEC to use the data from them to generate statistics to improve the voting experience, including for example, a prediction of queue waiting times based on the average elector flow through a polling place. This could be used to generate a live website feed so that electors can plan their time accordingly. This functionality should be considered in the further development of ECL technology.
- 2.47 The Committee is therefore recommending that ECLs be deployed to all pre-poll voting centres and mobile voting teams at the next federal election. This should be with a view to eventual universal implementation at subsequent elections. This will require a resourcing commitment.

Recommendation 1

The Committee recommends that the Australian Government adequately resource the Australian Electoral Commission to deploy electronic certified lists where possible to all pre-poll voting centres and to all mobile voting teams at the next federal election.

- 2.48 The cost of universally implementing ECLs based on trial costs with leased hardware is clearly prohibitive; however no dedicated work has been done on the cost of the AEC owning the hardware and therefore balancing the up-front cost over multiple elections. Nor has any detailed cost analysis been provided to the Committee on the potential cost savings generated by the reduced workload time and staff requirements for preliminary scrutiny when supported by ECLs. This work should be undertaken.
- 2.49 The Committee is also of the view that there may be more cost effective ways to develop this technology including shared use of infrastructure between jurisdictions. This would not only facilitate the sharing of resources but also support existing electoral roll harmonisation efforts.
- 2.50 This is also an area that could make use of an internet-based platform (rather than exclusive device-based software) so the existing networks in polling places (such as school and council computer systems) could be utilised.

- 2.51 The electoral roll can currently be accessed by a variety of stakeholders including elected Members of Parliament from any networked computer. There should be some capacity to extend this platform for use as an electronic certified list at an election.

Recommendation 2

The Committee recommends that, after the next federal election, the Australian Electoral Commission undertake a full cost benefit analysis of utilising electronic certified lists at all polling locations based on a permanent investment in the relevant technology and/or the development of a platform that can be accessed from any networked computer, with a view to full implementation at future elections.

Recommendation 3

The Committee recommends that the Special Minister of State propose to the states and territories that the further development of electronic electoral roll mark-off systems be undertaken in a collaborative approach to facilitate the sharing of resources.

- 2.52 Further, the Committee is aware that legislative change may be required to allow for the use of electronic certified lists as a form of approved list for marking electors who have been issued a ballot paper.

Recommendation 4

The Committee recommends that relevant sections of the *Commonwealth Electoral Act 1918* and the *Referendum (Machinery Provisions) Act 1984*, be amended to allow for the expansion of the use of electronic certified lists as a form of approved list for marking electors who have been issued a ballot paper.

Online enrolment

- 2.53 Electors now have the ability to enrol and update their enrolment details online. The AEC noted that:

At the 2013 election, more than 85 per cent of all enrolment transactions lodged by electors between announcement of the 2013 election on 3 August 2013 and close of rolls on 12 August 2013 occurred online through the AEC Online Enrolment Form (OEF).¹³

- 2.54 The ease of online enrolment/ update is considered a contributor to the increase in enrolment for the 2013 election,¹⁴ and in the 2013 close of rolls period the rate of online enrolment (534 451 persons) significantly outweighed the rate of enrolment by any other source (92 805 persons).¹⁵
- 2.55 The success and popularity of this online innovation indicates that voters feel confident engaging with the AEC online. These advances are important to continue to build confidence in the use of technology in relation to the electoral system.

Management of ballot papers

- 2.56 There are two areas in the management of ballot papers that could be assisted by technological investment:
- digital count; and
 - digital storage of ballot papers.

Digital count

- 2.57 A further opportunity to support the electoral process is to use scanning technology to both count and store ballot papers. The Australian Capital Territory (ACT) Electoral Commission uses a scanning system for the count of ballot papers and recommended it for its high degree of accuracy in the count:

On the counting side of things I think the Senate experience at the last election would get a lot more benefit out of our scanning system than it would out of our electronic voting system ... It is

13 AEC, *Submission 20.3*, p. 11.

14 AEC, *Submission 20.3*, p. 55.

15 AEC, *Submission 20.3*, p. 149. Other sources include division and post office issued forms (46 067); forms downloaded from the Internet (13 114); direct enrolment and update (10 037); State electoral (6 727); mail review and change of address notices (5 837); citizenship ceremonies (3 680); Transport authorities (1 380); other sources (5 963).

quite obvious that a scanning system that is using computers to verify that the preferences on ballot papers have been correctly recorded is far superior to a hand count of ballot papers even when looking at just single first preference above the line. A scanning system is going to give you a much more accurate count than a hand count will.¹⁶

- 2.58 Elections ACT officials scan all paper ballot papers and the votes are read by Intelligent Character Recognition software. Electoral officials check the computer interpretation against the paper ballot and make any required corrections.¹⁷ Scrutineers are able to observe all steps of this process.
- 2.59 The AEC also submitted that Optical Character Recognition (OCR) software and scanning hardware would be a good opportunity for investing in technology to aid counting processes.¹⁸ The ACT Electoral Commission has found a twofold effect of improved workforce management and the speed of the count:

An issue we found with data entry was that people with the skills to do data entry are getting harder and harder to find because it is not something that is out there in the larger workforce these days now that there is scanning and people are doing things directly online. There just is not a large casual workforce of people with data entry skills out there. So we decided at the 2008 election that we would use optical character recognition scanning. We also used that at the 2012 election. We were very pleased with the scanning system that we adopted at the last two elections. The speed with which we were able to get the count completed was pretty much the fastest that we could have completed it. In the ACT we are able to take postal votes up until the Friday after polling day – so six days after polling day – which means that you cannot strike the final count and do the final distribution of preferences until you have counted all the postal votes. Both in 2008 at 2012 we were able to finish the data entry of all the postal votes and error corrections of all the paper ballots on the Saturday after polling day. In 2008 we were able to finish the count in the middle of the afternoon on Saturday after election day. In 2012 we beat that by a few hours. We finished by about lunchtime on Saturday. That is

16 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, 29 July 2014, Canberra, p. 10.

17 Elections ACT, *Frequently asked questions*, accessed 28 October 2011 <elections.act.gov.au/elections_and_voting/electronic_voting_and_counting/faq>.

18 AEC, *Submission 20.3*, p. 76.

about as fast as you can count an election such as ours where you have to wait for postal votes.¹⁹

- 2.60 Greater accuracy in initial counting and scrutiny of votes, in potentially both House of Representatives and Senate elections, is an attractive prospect. The ACT Electoral Commissioner argued that accuracy is significantly improved in an electronic counting system:

I am saying a scanning system will give you a much more accurate count than a hand count will every time. If you look at the recount figures that are available on the AEC website, which simply lists those polling place total numbers that were counted in the first count and compared it to the total number of ballot papers counted in the second count, you see they made miscounts in every division in Western Australia and miscounts in more than half of the polling places, and we are just talking counting first preference votes above the line – single-ticket votes. Hand counting and hand sorting using humans alone is an error-prone thing. This is what we found in 1998. If you look at the result of the recount in Western Australia, you can see that hand counting even a single first preference on a ballot paper is something that human beings are not very good at. Computers are very good at it.²⁰

- 2.61 Efficiencies to be gained in scrutineer access to ballot papers and eventual storage of ballot papers are also a potential advantage.

- 2.62 The ACT Electoral Commissioner described the process the ACT uses to scan and scrutinise its ballot papers, whereby the system identifies and isolates ballot papers that are likely to require further scrutiny:

That is the point on which scrutineers are able to focus their attention, because they are the ballot papers that are not really straightforward. So what it does is: if you think of comparing that to a hand count, every now and then in a hand count you are going to come up against a tricky one that scrutineers will be interested in, but you have another 50 that are straightforward, so it is not isolated as being something that is worthy of attention. The way our system works is: it isolates all those ones that scrutineers are really interested in. So I actually think it is a much better system for scrutineering, from the parties' and the

19 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, 29 July 2014, Canberra, p. 5.

20 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, 29 July 2014, Canberra, p. 10.

candidates' point of view, because it really homes in on the ones that are worthy of attention.²¹

- 2.63 Part of the difficulty with scanning ballot papers currently is the size of the Senate ballot paper. The AEC submitted that there are machines available that are capable of scanning the current dimension of Senate ballot paper, but, due to the size of the ballot paper, this technology is expensive and therefore unlikely to be able to be implemented at every polling place.²²
- 2.64 Nonetheless, if a solution could be found for digitising ballot papers prior to any movement from a polling place, this would provide a solution to the ballot transport errors that occurred during the 2013 WA Senate election. The Committee also notes that if the recommendations of its first interim report are adopted, this should significantly reduce the size of the Senate ballot paper.
- 2.65 Australia Post submitted that there is current scanning and data capture technology that could support scanning and digitisation at various stages of the count process:

There are four distinct stages in the count process that provide an opportunity for scanning and digitisation of electoral forms and associated content. Scanning has more benefits the earlier the stage selected, however associated costs would increase with a requirement for more infrastructure at those earlier stages.

- The initial count: providing scanning and assessment of each vote as part of the initial count (performed the night of the vote). Scanning could be performed at each polling place and would benefit from a large amount of scrutiny, and any mismatches in total vote counts will automatically be identified and assessed. Additionally, the risk of ballots being 'lost' before digitisation will be minimised.
- The scrutiny count: providing scanning and assessment of each ballot as part of the fresh scrutiny (performed the Monday after the vote). A digital representation of all votes could be created for future reference.
- The recount process: providing scanning and assessment of each ballot where a recount process is initiated. As part of this, ballots could be assessed at either an AEC premises or one of Australia Post's secure specialist processing facilities (physically supervised by scrutineers if necessary). This process could incorporate an additional count of disputed ballots, ensuring an accurate count, and could possibly be cross

21 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, 29 July 2014, Canberra, p. 12.

22 Tom Rogers, a/g Electoral Commissioner, *Transcript of Evidence*, 31 July 2014, Canberra, p. 14.

referenced against available voter rolls. It would not, however, identify ballots that had gone ‘missing’ between the place of voting and the place of scrutiny.

- After the declaration of results: conducting high speed scanning of all ballots at Australia Post facilities. This could be pursued to provide a backup of the vote for archival purposes after the vote has been completed.²³

- 2.66 Models of scanning and counting of ballot papers are also utilised in international jurisdictions. While the ACT utilises the technology at the counting stage, in some Canadian jurisdictions the voter feeds their ballot paper through a scanner as part of the act of depositing the paper in a ballot box. The vote is immediately recorded and votes are tallied after the close of polls.²⁴
- 2.67 In recent elections in New Brunswick, Canada, the Canadian leader in the use of this technology²⁵ some concerns were raised about this method of scanning and counting ballot papers, namely:
- As a vote is scanned, the machine ‘beeps’ if a person has not correctly completed their ballot paper and it has been argued that this violates the secrecy of the vote for those who actively choose not to complete or to ‘spoil’ their ballot paper; and²⁶
 - Scrutineers are not able to observe the count as it occurs as an individual is voting and there is no way to verify the vote is accurately scanned without compromising the secrecy of the ballot.²⁷
- 2.68 These issues can be managed in the Australian context, as long as the principle of an open and transparent electoral system is kept at the core of any developments.
- 2.69 The experience of these jurisdictions raises important issues for consideration prior to any wholesale adoption of this technology. As is discussed in Chapter 3, international jurisdictions that have implemented electronic voting have found that an auditable paper trail is an essential component of any electronic voting system to ensure trust in the system.

23 Australia Post, *Submission 174*, p. 9.

24 Elections New Brunswick, *Frequently asked questions: technology*, accessed 28 October 2014, <www1.gnb.ca/elections/en/faq/faq-e.asp?CATEGORYID=5&TYPE=1>.

25 Elections Canada, ‘The New Brunswick Model’, accessed 29 October 2014, <elections.ca/content.aspx?section=res&dir=cons/comp/crfr&document=d&lang=e>.

26 *The Voting News*, ‘Canada: New Brunswick voting machines erode secrecy of spoiled ballots’, accessed 28 October 2014, <thevotingnews.com/new-brunswick-voting-machines-erode-secrecy-of-spoiled-ballots-cbc-news>.

27 Antony Green, *Electronic tabulation problems at New Brunswick election*, accessed 28 October 2014 <blogs.abc.net.au/antonygreen/2014/09/electronic-tabulation-problems-at-new-brunswick-election>.

Likewise, scanning technology must be able to be scrutineered without in any way affecting the right to a secret ballot.

Digital storage

- 2.70 Currently, Senate ballot papers need to be stored for the life of Senate terms (approximately 7 years in total), which is not an insubstantial logistical and security requirement. If scanned images of the ballot papers were acceptable in place of the physical papers, this could result in storage cost savings as well as being kept indefinitely.
- 2.71 Such optimisation would also align with the Commonwealth's e-government focus, the priorities of the *Australian Public Service ICT Strategy 2012-2015*, and the Australian Government's Digital Transition Policy, which requires all agencies to move to digital records keeping.²⁸
- 2.72 Section 393A of the Electoral Act provides for the preservation and custody of ballot papers after an election. For the purposes of this section, ballot papers become 'electoral documents', along with certified lists, declaration envelopes and other election-related items.
- 2.73 Current records destruction authority, expressed in the Normal Administrative Practice outlined in section 24 of the *Archives Act 1983* and exercised by General Records Authorities issued by Archives, along with the relevant Records Authorities issued to the AEC for the destruction of election, ballot and referendum materials²⁹ are currently silent on digital versions of ballot papers in respect of the current requirements for storage of 'electoral documents'.
- 2.74 In this regulatory context the digital storage of ballot papers requires careful consideration, as the legal status of scanned images of ballot papers would need to be determined. Original paper ballots would also need to be kept for a suitable period of time after the declaration of polls and the period for potential Court of Disputed Returns challenges has lapsed.
- 2.75 Nonetheless, the storage of scanned ballot papers could offer real benefit in terms of the savings associated with long-term leasing of storage facilities.

28 The strategy is viewable at <finance.gov.au/policy-guides-procurement/ict_strategy_2012_2015/>, the Digital Transition Policy is outlined at <naa.gov.au/records-management/digital-transition-and-digital-continuity/digital-transition-policy/index>.

29 Records Authorities can be accessed at <naa.gov.au>.

Committee comment

- 2.76 The Committee supports the evolution of electronic support for the federal electoral process, and believes the most immediate and tangible benefits are likely to be gained in digitising facets of this process.
- 2.77 The successful use of online enrolment/update is also supported. These applications harness existing, secure technology in order to enhance the integrity of the electoral process.
- 2.78 The introduction of electronic counting, scanning and storage of ballot papers (along with expanding the use of ECLs) offers potential for a quicker process with greater accuracy, harnessing existing technology. Use of this technology will not only support the electoral process, but, as with ECLs, has the potential to assist in building community confidence in the use of technology for elections.
- 2.79 There is little risk associated with scanning ballot papers, indeed, it will be an enhancement by providing a further verification process to the manual count.
- 2.80 The Committee is therefore recommending that the AEC develop and trial electronically-assisted counting of ballot papers at all pre-poll voting centres at the next federal election. This should be with a view to expansion as widely as possible at future elections.
- 2.81 Any use of technology in association with the electoral process must have the principle of the sanctity of the ballot at its core, including upholding the right to a secret ballot and ensuring transparency in the counting process.

Recommendation 5

The Committee recommends the Australian Electoral Commission develop and trial the electronically-assisted counting of ballot papers at all pre-poll centres for the next federal election.

- 2.82 Further, if ballot papers are to be scanned, it may be possible to store digital ballot papers rather than paper ballots which may lead to a considerable saving for the Government in terms of expenditure on storage facilities. The Committee considers this proposal warrants further investigation, which may include amendments to the Electoral Act.

Recommendation 6

The Committee recommends that the Australian Government investigate the feasibility of digital storage of scanned ballot papers to replace storage of paper ballots.

National and international experience

- 3.1 By 2009, the internet was the most common way that Australians made contact with government.¹ In this digital era, Australians are an increasingly mobile and technologically-engaged population, and this has led to expectations of flexibility, convenience and immediacy.
- 3.2 Given the events that occurred during the 2013 federal election, it is not surprising that a common response has been a call for electronic voting.
- 3.3 A number of jurisdictions, both in Australia and internationally, have trialled electronic voting. These trials have covered both static and internet voting. There has been mixed success with these trials, and while some jurisdictions continue to expand electronic voting, the majority have chosen to abandon the technology over concerns about the security and sanctity of the ballot.
- 3.4 This chapter outlines national and international experiences with electronic voting. It explores both the success of these systems and the widespread academic and community criticisms.

Australian jurisdictions

- 3.5 There has been no consistent development of electronic voting across the Australian jurisdictions, and no clear consensus on moving towards it. Until this occurs, there are challenges for the successful adoption of electronic voting on a national scale.

1 Electoral Council of Australia and New Zealand (ECANZ), 10 September 2013, *Internet voting in Australian election systems*, p. 34, accessed 26 August 2014, <eca.gov.au/research/files/internet-voting-australian-election-systems.pdf>.

- 3.6 In a paper prepared for the NSW Electoral Commission (NSWEC), Professor Rodney Smith of the University of Sydney found that there were eight factors which appeared to affect the adoption of electronic voting:

The first three are patterns of elite, interest group and mass support. The next two relate to the use of information technology in everyday life and in other aspects of elections. The sixth is administrative capacity. The seventh is the relationship between electronic voting and existing voting. The last is the staged introduction of electronic voting.²

- 3.7 It is important to acknowledge these factors as the context for the evolution of electronic voting. At a federal level, only elements of these factors have been achieved or are currently in play in relation to the future development and implementation of electronic voting.
- 3.8 Currently, a number of systems of electronic voting or electronic support for voting are utilised at various levels in Australia. Processes and lessons from these are important factors in building capacity in electoral administration and confidence in voters, and will help inform next steps into the future.

Federal elections

- 3.9 Currently at the federal level there is only one form of electronic voting of any type – the assisted telephone voting system for blind or low vision voters.
- 3.10 In this system, a voter with blind or low vision registers to vote using the system and is issued with a de-identified registration number and personal identification number. Using these details, the voter can telephone into the system and is then transferred to an operator who does not know the voter's identity. The operator interacts with the voter and records their vote.
- 3.11 This system was developed in consultation with a peak-body reference group, and has been commended by the recently outgoing Disability Commissioner. However, there is still concern in the blind or low vision community that the current system does not allow for a completely secret ballot, as users are still required to provide their candidate preferences to a third party.³

2 R Smith, July 2009, *International Experiences of Electronic Voting and Their Implications for New South Wales*, p. 3, NSW Electoral Commission (NSWEC), Sydney, accessed 13 November 2014, <elections.nsw.gov.au/__data/assets/pdf_file/0013/103207/International_Experiences_of_Electronic_Voting_and_Their_Implications_for_New_South_Wales_Report_2009.pdf>.

3 Australian Electoral Commission (AEC), *Submission 20.3*, p. 61.

- 3.12 Vision Australia supports the assisted telephone voting system, 'but only as part of a suite of broader options for accessible voting – in particular, internet voting and phone computerised voting, such as the iVote system' (discussed below).⁴
- 3.13 Vision Australia proposed that:
- ... like the iVote system in New South Wales, any broader options for accessible voting be made more generally available, which makes them more economically viable if they are rolled out to a larger number of people, and particularly other categories of voters that might have literacy or access issues, people with disability, people who live certain distances from polling places or people who might be out of the country on polling day.⁵
- 3.14 In response to past calls for a more extensive electronic voting system and a recommendation from a previous Electoral Matters Committee, a federal trial of an alternative electronically-assisted voting for blind or low vision voters and a remote electronic voting trial for Australian Defence Force (ADF) personnel was undertaken for the 2007 federal election using static kiosks.⁶
- 3.15 The 2007 blind or low vision trial was restricted in scope to 30 pre-poll voting sites, and to electors who were sight impaired such that they were unable to vote without assistance. The kiosks were available in the pre-poll voting period, and on election day. The government also required that the output from the kiosks be a printed record for later inclusion in the count, making the solution a voting 'aid' rather than a system that resulted in electronic capture of vote data.
- 3.16 The solution adopted was based on a desktop computer format, with a 53 centimetre flat screen monitor, a telephone-style keypad and earphones. The computer itself was encased in a tamper-evident perspex case. While voters with some sight could be guided through the voting process using the information on screen, those without sight were guided by comprehensive instructional voice scripts.⁷
- 3.17 The Electoral Council of Australia and New Zealand (ECANZ) report on internet voting outlined the 2007 trial:

4 Vision Australia Ltd and Blind Citizens, *Transcript of Evidence*, 15 April 2014, Melbourne, p. 49.

5 Vision Australia Ltd and Blind Citizens, *Transcript of Evidence*, 15 April 2014, Melbourne, p. 49.

6 Joint Standing Committee on Electoral Matters, *Report of the Inquiry into the conduct of the 2004 federal election and matters related thereto*, September 2005, pp. 257-272.

7 ECANZ, 10 September 2013, *Internet voting in Australian election systems*, p. 22, accessed 26 August 2014, <eca.gov.au/research/files/internet-voting-australian-election-systems.pdf>.

A total of 850 votes were cast over 29 locations during the two week voting period. The kiosk was the first of its kind to use a telephone style keypad interface, which drew parallels with the rules of telephone banking. This bridged the gap between voters who were unfamiliar with using a computer but were familiar with telephones, ATMs or telephone banking. The trial demonstrated that electronic voting for the blind or low vision community could provide an intuitive, secure, secret and independent method of voting. It also highlighted that an “audio assisted voting system” could potentially provide benefits for any voter who requires assistance with the printed ballot format.⁸

- 3.18 The ADF voting trial was undertaken on computers connected to the Defence Restricted Network. However, as the resultant votes were still printed and included in the final manual paper count, this trial was also a voting ‘aid’, and cannot properly be considered an electronic voting system such as that used in the Australian Capital Territory (ACT).⁹
- 3.19 While both systems were commended for their access improvements, they were both costly per vote:
- The combined costs of the trials was over \$4 million, with an average cost per vote cast of \$2,597 for the trial of electronically assisted voting for blind and low vision electors and \$1,159 for the remote electronic voting trial for selected defence force personnel serving overseas. This compares to an average cost per elector at the 2007 election of \$8.36.¹⁰
- 3.20 These particular voting methods have not been continued at subsequent elections on recommendation from the Electoral Matters Committee of the 42nd Parliament.¹¹

New South Wales

- 3.21 In 2011 the NSWEC implemented a remote telephone and internet voting system known as iVote. This was the first of its kind used in Australia, and allowed voters to register on the internet or by phone to utilise the system.

8 ECANZ, 10 September 2013, *Internet voting in Australian election systems*, pp. 22-23, accessed 26 August 2014, <eca.gov.au/research/files/internet-voting-australian-election-systems.pdf>.

9 ECANZ, 10 September 2013, *Internet voting in Australian election systems*, p. 23, accessed 26 August 2014, <eca.gov.au/research/files/internet-voting-australian-election-systems.pdf>.

10 Joint Standing Committee on Electoral Matters, March 2009, *Report on the 2007 federal election electronic voting trials*, Canberra, p. iii.

11 Joint Standing Committee on Electoral Matters, March 2009, *Report on the 2007 federal election electronic voting trials*, Canberra.

- 3.22 The system was designed to cater for blind or low vision voters, voters who were disabled within the meaning of applicable anti-discrimination legislation, and voters who were more than 20kms from a polling place on election day. Eligibility was later expanded to include any voter who was not within New South Wales (NSW) on election day.
- 3.23 More than 51 000 voters registered for the iVote service and nearly 47 000 of those voted using the service. Of those who voted, 1.43 per cent qualified to use the service by virtue of being blind or vision impaired; 2.77 per cent because of other disabilities; 3.51 per cent because they lived in remote rural areas; and 92.3 per cent because they were outside NSW.¹²
- 3.24 All votes taken were stored in central servers in two data centres. At the close of the poll the votes were printed and included in the count at the electoral district level. The iVote system has been successfully used at a number of by-elections since the 2011 State election,¹³ most recently those held for the District of Northern Tablelands and Miranda in 2013, and Charlestown and Newcastle in 2014.¹⁴
- 3.25 The iVote system is distinct from the current assisted telephone voting system used for blind or low vision voting federally, as the voter enters their vote into a completely automated telephone system, without the requirement to reveal their vote to another person, de-identified or otherwise.
- 3.26 While the iVote system is relatively secure, due to the fact that it utilises telephone systems for blind or low vision voting transactions and encrypted internet data architecture, the vote data on the voter's computer or in the NSWEC's servers is still open to potential manipulation.¹⁵
- 3.27 In response to criticisms of the system's security, the NSWEC has commissioned a third-party provider to strengthen the security of the system software prior to the 2015 state election, along with other hardware and data transmission improvements.¹⁶

12 Allen Consulting Group (2011), *Evaluation of Technology Assisted voting provided at the New South Wales State General Election March 2011*, NSW Electoral Commission, Sydney, p. 20, accessed 6 August 2014, <elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports>.

13 NSW Electoral Commission, *iVote*, accessed 17 November 2014, <elections.nsw.gov.au/voting/ivote>

14 By-election results and the numbers of iVote votes received can be viewed at <elections.nsw.gov.au/past_results/by_elections>.

15 Rajeev Gore and Vanessa Teague, *Submission 114*, p. 13.

16 J Taylor, 'NSW e-voting shuns perfection for good, practical security', *ZDNet*, 21 May 2014, accessed 29 August 2014, <zdnet.com/au/nsw-e-voting-shuns-perfection-for-good-practical-security-7000029703/>.

Australian Capital Territory

- 3.28 The ACT was the first jurisdiction to use an electronic voting system for parliamentary elections with a trial in the 2001 ACT Legislative Assembly election.
- 3.29 Following the trial, the ACT Electoral Commission acknowledged how a move to electronic voting would change the nature of elections, and recommended that the ACT Government consider:
- moving away from the traditional concept of “polling day” and replacing it with a “polling period” which could be from 1-3 weeks. By extending the right to vote throughout a polling period to all electors, electronic voting could be made available at (say) 12 locations strategically placed near main shopping centres and workplaces. Rather than concentrating voting on 1 day at local polling places, electors could vote over (say) a 3 week period at a regional voting centre. In this way, electronic voting could be made available to almost all electors.¹⁷
- 3.30 Electronic voting – in pre-poll centres, including on election day – has been used at all subsequent ACT elections in 2004, 2008 and most recently in 2012. Approximately 25 per cent of all ACT voters used electronic voting at the 2012 election.¹⁸
- 3.31 The ACT’s electronic system uses standard personal computers as voting terminals in polling booths, with voters using a barcode to authenticate their votes. The same system, with incremental upgrades to the open source code and software, has been used at all ACT elections since 2004. At the 2012 election the system featured at six locations across Canberra’s main town centres (being the pre-poll centres that became polling booths on election day).¹⁹
- 3.32 Voting terminals are linked to a server in each polling location using a secure local area network. No votes are taken or transmitted over a public network such as the internet or local area Wi-Fi network.²⁰ The ACT Electoral Commissioner argued that it would be very difficult to remotely

17 Elections ACT, June 2002, *The 2001 ACT Legislative Assembly election electronic voting and counting system review*, Canberra, p. 3, accessed 14 July 2014, <elections.act.gov.au/__data/assets/pdf_file/0007/1798/2001electionreviewcomputervoting.pdf>.

18 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, Canberra, 29 July 2014, p. 2.

19 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, Canberra, 29 July 2014, p. 2.

20 Elections ACT, *Electronic Voting and Counting*, accessed 1 July 2014, <elections.act.gov.au/elections_and_voting/electronic_voting_and_counting>.

- hack the system as it would require gaining physical access to locked servers in locked polling booths.²¹
- 3.33 The source code for the system is publicly available in the interests of transparency and study purposes, but also to allow for interested parties to test the system and aid in identifying issues.²²
- 3.34 For those who do vote electronically in the ACT, there is a high degree of confidence in the system. An exit poll of voter satisfaction after the 2004 election showed that 86 per cent of voters who used electronic voting found it easy to use; 88 per cent thought the system fast and efficient; and 83 per cent thought the system had clear instructions.²³
- 3.35 Electronic voting is only available in the ACT in six pre-poll locations.²⁴ The ACT is a small jurisdiction, both in terms of population and geography, and so the hardware requirements are therefore also small compared to that which would be required to implement this system nationally.

International experience

- 3.36 As in Australia, there is no international consensus on standards of electronic voting technology, implementation or regulation. As Thomas Buchsbaum, a European expert on electronic voting, has noted:
- No universal trend towards a definite introduction of e-voting can be detected, not even by countries where first steps were undertaken on such a way.²⁵
- 3.37 While a number of countries have conducted electronic voting pilots of various kinds, the majority continue to rely on paper-based voting methods for their government elections.

21 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, Canberra, 29 July 2014, p. 2.

22 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, Canberra, 29 July 2014, pp. 8-9.

23 Elections ACT, *Electronic voting and counting system: review 2004*, June 2005, p.14, accessed 14 July 2014, <elections.act.gov.au/__data/assets/pdf_file/0006/1797/2004electionreviewcomputervoting.pdf>.

24 Phillip Green, ACT Electoral Commission, *Transcript of Evidence*, 29 July 2014, Canberra, p. 6.

25 T Buchsbaum, 2004, 'E-Voting: International Developments and Lessons Learnt', in A Prosser and R Krimmer (eds), *Electronic Voting in Europe – Technology, Law, Politics and Society*, Proceedings of the Workshop of the ESF TED Programme Together with GI and OCG, Bonn, GI-Edition p. 41.

- 3.38 The evolution of electronic voting has been a long process over many decades, but there are still no clear platforms or programs that have been proven to give a definitive answer to modernising voting processes.
- 3.39 The development of electronic voting and support systems will often occur as a result of a desire of electoral authorities to enable dispersed populations to vote in an easier manner (such as in Estonia), a desire to modernise processes to appeal to voter populations (such as in Ireland or the United States), or to enable easier voting and counting due to size of the population (such as in India).
- 3.40 Two countries – Brazil and Estonia – have gone beyond trial phases and have implemented universal use of electronic voting machines within polling locations or remote internet voting. Ireland and The Netherlands have also made significant investment in electronic voting, but have since abandoned its use, and jurisdictions in the United States are facing difficulties with aging infrastructure and increasing maintenance costs.

Brazil

- 3.41 Brazil has had full isolated static electronic voting using electronic machines since its 2000 election and has not faced many direct challenges since. However, this is changing as time progresses and civil society and other non-governmental organisation oversight groups question the transparency and verifiability of the voting system implemented by Brazil's electoral authority, the Tribunal Superior Eleitoral (TSE).²⁶
- 3.42 The development of the Brazilian electronic voting system has been driven by a compulsory voting system, low literacy rates, and a need to support multiple tiers of elections. The machine utilises a numeric keypad that is supported by a screen that displays a picture of the candidate voted for.²⁷
- 3.43 Voters are presented with a stub to prove they have voted and the data from the machines is captured on a hard memory storage device that can be uploaded to a central counting program and database. This system is well supported in the community, as it vastly speeds up the counting and results in Brazilian elections (where there can be thousands of candidates) compared to the previous paper ballot system. It significantly reduces the spoiled and informal ballot paper rate experienced previously, as well as widely-reported ballot paper tabulation fraud.²⁸

26 National Democratic Institute, *Overview of Brazil case study*, accessed 19 August 2014, <ndi.org/e-voting-guide/brazil-CS/overview>.

27 *BBC News*, 1 October 2008, 'How Brazil has put an 'e' in vote', accessed 20 August 2014, <news.bbc.co.uk/2/hi/7644751.stm>.

28 National Democratic Institute, *Brazil: Decision making process on electronic voting*, accessed 20 August 2014, <ndi.org/e-voting-guide/brazil-CS/decision-making-process>.

- 3.44 The simplicity of the voting machine is also supported by the party list and first-past-the-post systems used for the Brazilian Chamber of Deputies and Federal Senate elections.
- 3.45 Development of the electronic system in Brazil was unusual in that there was little call for a system to be developed. Instead, the TSE proactively established a feasibility committee that researched and developed the system, independent of much community or wider expert engagement. This independent development has often drawn criticism, which has highlighted Brazil's large expenditure on information technology in voting, health and procurement without any measurable increase in trust or an equivalent increase in benefit to the population most at need of government support.²⁹
- 3.46 The electronic system in Brazil seems to serve the Brazilian electoral context well, although the security and transparency of the system is still subject to criticism.
- 3.47 The National Democratic Institute has outlined a number of key points arising from the Brazilian experience:
- any system needs to be independently auditable and verifiable, with a clear dispute resolution mechanism;
 - source code for electronic systems should be vetted and open to interrogation;
 - paper audit trails are crucial to enabling challenges and building transparency;
 - open access to security system development by academics and groups interested in transparency builds essential trust in the system;
 - security systems must be built to withstand external as well as internal attacks; and
 - inclusive development and voter education is important to build trust.³⁰

Estonia

- 3.48 Estonia offers remote internet voting to the entire electorate during the pre-poll period. Based on the 2011 election, up to 25 per cent of

29 J Filho, 2009, 'E-Voting and the Creation of Trust for Socially Marginalized Citizens in Brazil', *Journal of Democracy and Open Government*, accessed 20 August 2014, <jedem.org/article/view/26>, p. 187.

30 National Democratic Institute, *Brazil: Lessons learned*, accessed 20 August 2014, <ndi.org/e-voting-guide/brazil-CS/lessons-learned>.

- participating Estonian electors vote online, making it the world's largest internet democratic process.³¹
- 3.49 Estonians have had the ability to vote online since 2005, and an essential part of the system is the existence of a national ID card which also acts as a smartcard that can be used for online identity verification.
- 3.50 Estonia has a long history of electronic engagement by government and is considered to be a highly technologically literate nation. With high investment in e-commerce and government, as well as computer literacy in education from the early 2000s, Estonia was an ideal environment for electronic democratic processes to evolve.³²
- 3.51 Yet the Estonian system has not been without criticism, especially in relation to potential security failings and vulnerabilities with identity verification using the national ID card.³³
- 3.52 The internet voting platform allows voters to vote multiple times from home or other remote computers using their ID card as authentication. Voters are allowed to download the voting application, vote using the application, and then send back the vote data with a digital signature as verification/declaration of the vote's authenticity.³⁴
- 3.53 The ability to vote multiple times, with the last electronic vote or a valid paper vote being the only one counted, is a system theory design to enable people who may have been coerced into voting a particular way to change their vote once the coercion has ended.³⁵
- 3.54 A 2014 analysis of the Estonian voting system found serious security and data integrity flaws and recommended the immediate withdrawal of the system. The major findings were:
- The security architecture underpinning the Estonian platform is perilously out of date and is not able to deal with state-level cyber-attacks or concentrated hacking attempts from other entities.

31 J Halderman et al, May 2014, *Security analysis of the Estonian internet voting system*, accessed 27 August 2014, <estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf>.

32 Freedom House, *Estonia*, accessed 20 August 2014, <freedomhouse.org/report/freedom-net/2012/estonia>.

33 L Constantin, 'Estonian electronic voting system vulnerable to attacks, experts say', *CIO*, 13 May 2014, accessed 19 August 2014, <cio.com.au/article/544862/estonian_electronic_voting_system_vulnerable_attacks_researchers_say/>.

34 National Democratic Institute, *Internet voting in Estonia*, accessed 21 August 2014, <ndi.org/e-voting-guide/examples/internet-voting-in-estonia>.

35 J Halderman et al, May 2014, *Security analysis of the Estonian internet voting system*, accessed 27 August 2014, <estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf>.

- The platform relies heavily on voters' computer and relevant security software. As soon as the software control on data is taken away from the electoral authority, the confidence in vote data, and therefore results, is undermined.
- The operation of the platform by election staff highlighted lapses in operational security and procedures that exposed vote data to manipulation, or inadvertently released security personal identification numbers (PINs) and passwords.
- Replicated software platforms were easily hackable and results could be changed or removed without trace, or viruses and malicious software could be installed on systems easily, including 'bot' software that could make a voter believe they had cast their vote but then replace that vote data with other fraudulent data.
- Full disclosure and transparent processes were lacking, resulting in a lack of trust in the system.³⁶

3.55 The report concluded that:

Compared to other online services like banking and ecommerce, voting is an exceedingly difficult problem, due to the need to ensure accurate outcomes while simultaneously providing a strongly secret ballot ... Based on our tests, we conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes. Short of this, there are abundant ways that such an attacker could disrupt the voting process or cast doubt on the legitimacy of results ...

Due to these risks, we recommend that Estonia discontinue use of the I-voting system. Certainly, additional protections could be added in order to mitigate specific attacks, but attempting to stop every credible mode of attack would add an unmanageable degree of complexity. Someday, if there are fundamental advances in computer security, the risk profile may be more favorable for Internet voting, but we do not believe that the I-voting system can be made safe today.³⁷

3.56 The Estonian National Election Committee has denied the findings and assertions of the report, claiming that their system is secure and that 'online balloting allows us to achieve a level of security greater than what

36 Independent Report on E-voting in Estonia, *Our Findings*, accessed 20 August 2014, <estoniaevoting.org/findings/>.

37 J Halderman, et al, May 2014, *Security analysis of the Estonian internet voting system*, accessed 27 August 2014, <estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf>, p. 11.

is possible with paper ballots'.³⁸ However, the report's authors have countered this response, stating that the weaknesses of the system as identified are correct and that discourse on the ongoing security of the system needs to continue.³⁹

- 3.57 Notwithstanding the Estonian National Election Committee's defence of its internet voting system, the Organisation for Security and Cooperation in Europe observation of the 2011 election also raised concerns with the security, transparency and verifiability of the system.⁴⁰
- 3.58 There has not been a national election in Estonia since these criticisms were published; the next Estonian national election is due in 2015.

Ireland

- 3.59 Ireland invested heavily in electronic voting machines from 1999 and was scheduled to introduce this form of voting nationwide in June 2004, but abandoned these plans in May 2004 due to questions about cost and the accuracy and secrecy of the ballot.⁴¹
- 3.60 The Irish Commission on Electronic Voting found that it was not possible to express confidence in the use of electronic voting due to the ongoing testing of software:
- as changes are made to the system, each new software version needs to be reviewed and tested in full before it can be relied upon for use in real elections;
 - it has not been possible for the Commission to review the impact of the changes made in successive versions of the software in time for inclusion in this report; and
 - the fact that new versions of the software continue to be issued in the run-up to the June elections is unsatisfactory.⁴²
- 3.61 The Irish system was further undermined by the fact that computer scientists were able to prove vulnerabilities in the security of the systems.⁴³

38 National Election Committee of Estonia, 13 May 2014, *Comment on the article published in The Guardian*, accessed 11 November 2014, <vvk.ee/valimiste-korraldamine/vvk-uudised/vabariigi-valimiskomisjoni-vastulause-the-guardianis-ilmunud-artiklile/>.

39 Independent Report on E-voting in Estonia, *Our Response to the National Election Committee's Statement*, accessed 11 November 2014, <<https://estoniaevoting.org/press-release/response-national-election-committees-statement/>>.

40 Office for Democratic Institutions and Human Rights, 16 May 2011, *OSCE/ODIHR Election Assessment Mission Report*, pp. 8-15.

41 C MacCárthaigh, Irish Citizens for Trustworthy E-voting, *Electronic voting in Ireland*, accessed 3 October 2014, <stdlib.net/~colmmacc/e-voting-ireland.pdf>.

42 As quoted in *The Register*, 30 April 2004, 'Ireland to scrap e-voting plan: Accuracy and secrecy in question', <theregister.co.uk/2004/04/30/ireland_evote/> accessed 3 October 2014.

43 Rajeev Goré, *Transcript of Evidence*, 26 March 2014, Canberra, p. 7.

3.62 Ongoing testing of software contributed to the increasing cost of the system. At the time of abandoning the trial, the responsible minister stated that:

It is clear from consideration of the Report of the Commission on Electronic Voting that significant additional costs would arise to advance electronic voting in Ireland. This decision has been taken to avoid such costs, especially at a time of more challenging economic conditions. The financial and other resources that would be involved in modifying the machines in advance of implementation could not be justified in present circumstances ... the public in broad terms appear to be satisfied with the present paper-based system and we must recognise this in deciding on the future steps to be taken with the electronic voting system ... 'the assurance of public confidence in the democratic system is of paramount importance and it is vital to bring clarity to the present situation.'⁴⁴

3.63 Ireland made a significant investment in its electronic voting system and its failure has been costly. Against an initial investment of €51 million in the machines and storage costs of €3.2 million, the machines were sold for scrap recouping just €70 267 for the state.⁴⁵

3.64 The waste associated with the investment in electronic voting has been roundly criticised. On announcing the disposal of the machines, the Environment Minister labelled the investment 'ill-conceived and poorly planned' and a 'scandalous waste of public money.'⁴⁶

3.65 Ireland has since passed legislation banning electronic voting⁴⁷ after members of the parliament's public account committee referred to electronic voting as a 'dead-duck' and suggested that the only worth of the machines was as items for sale on the memorabilia market.⁴⁸

44 Department of Environment, Community and Local Government (Ireland), Media Release, *Minister Gormley announces Government decision to end electronic voting and counting project*, 23 April 2009, accessed 3 October 2014, <environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm>.

45 P Melia and L Byrne, '€54m voting machines scrapped for €9 each', *Irish Independent*, 29 June 2012, accessed 3 October 2014, <independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212>.

46 P Melia and L Byrne, '€54m voting machines scrapped for €9 each', *Irish Independent*, 29 June 2012, accessed 3 October 2014, <independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212>.

47 Rajeev Goré, *Transcript of Evidence*, 26 March 2014, Canberra, p. 7.

48 F Sheahan, 'Sell dud e-voting machines to pubs as scrap, say TD', *Irish Independent*, 28 April 2006, accessed 3 October 2014, <independent.ie/irish-news/sell-dud-evoting-machines-to-pubs-as-scrap-say-tds-26391467>.

The Netherlands

3.66 Following the Irish experience, the Netherlands also reversed its movement to electronic voting after decades of development. The Netherlands has used voting machines in some form since 1965 and the implementation of electronic voting was widely supported:

By 2006, 99 percent of municipalities were using electronic voting machines for national and local elections. Expatriates could vote using the internet and Dutch electoral authorities were planning to allow internet voting within the Netherlands. Electronic voting was popular. Surveys indicated that more voters trusted electronic voting machines than trusted paper ballots. Among expatriate internet voters, 99 percent liked the experience and 95 percent would use it again.⁴⁹

3.67 The Dutch Government reverted back to a purely paper-supported system after a group of computer scientists:

used their technical skills to demonstrate that, among other things, the machines were not physically or technically secure and could be manipulated to alter the results of elections without detection.⁵⁰

3.68 The subsequent official commission, reviewing the use of electronic voting, found various government failings including:

- voting machines did not receive enough attention;
- the Ministry of Interior lacked technical knowledge, resulting in officials becoming overly dependent on external actors, including technology vendors; and
- the government did not react to signs that should have raised concern.⁵¹

3.69 The report further found that:

certification and testing of the voting machines was based on outdated standards and that reports from these tests should have been made public. The report noted that the legal framework did

49 R Smith, July 2009, *International Experiences of Electronic Voting and Their Implications for New South Wales*, NSWEC, Sydney, accessed 13 November 2014, <elections.nsw.gov.au/__data/assets/pdf_file/0013/103207/International_Experiences_of_Electronic_Voting_and_Their_Implications_for_New_South_Wales_Report_2009.pdf>, p. 16.

50 R Smith, July 2009, *International Experiences of Electronic Voting and Their Implications for New South Wales*, NSWEC, Sydney, accessed 13 November 2014, <elections.nsw.gov.au/__data/assets/pdf_file/0013/103207/International_Experiences_of_Electronic_Voting_and_Their_Implications_for_New_South_Wales_Report_2009.pdf>, p. 17.

51 National Democratic Institute, undated, *Re-evaluation of the use of electronic voting in the Netherlands*, accessed 3 October 2014, <ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands>.

not adequately address the specifics of electronic voting, particularly the security requirements.⁵²

- 3.70 In 2008 the Dutch Government passed a law banning the future use of electronic voting.⁵³

United States of America

- 3.71 In the United States (US), the experience with electronic voting has been mixed.
- 3.72 Electronic voting increased in the years after the controversial 2000 presidential election. Electronic voting was considered to be a solution to the problems encountered with manual voting machines, such as the chad-punching machines used in Florida that led to the eventual US Supreme Court ruling awarding the Florida Electoral College votes to George W Bush. Electronic voting was also seen as a solution to voter comprehension issues with differing and complicated ballot papers.
- 3.73 US electoral authorities made a large original investment in e-voting machines in 2002, facilitated by the *Help America Vote Act* 2002 passed by the US Congress. However, this rapid advance into electronic-only systems was undermined by the lack of an auditable paper trail. By 2008 many states required paper trails to ensure the veracity of votes cast and greater transparency in the system, rendering many of the originally purchased machines obsolete. As of 2010, 40 states had moved towards requiring paper trails.⁵⁴
- 3.74 Further, as shown by the 2014 mid-term elections in the US, there has been a movement away from the electronic voting systems introduced in the 2000s due to concerns with ageing equipment and security.⁵⁵

52 National Democratic Institute, undated, *Re-evaluation of the use of electronic voting in the Netherlands*, accessed 3 October 2014, <ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands>.

53 J Libbenga, 'Dutch ban voting computers over eavesdropping fear', *The Register*, 20 May 2008, accessed 1 September 2014, <theregister.co.uk/2008/05/20/dutch_ban_on_voting_computers/>.

54 International IDEA, *Introducing Electronic Voting: Essential Considerations*, p. 25, accessed 22 August 2014, <http://www.idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>. The paper audit trail is often referred to as a Voter Verifiable Paper Audit Trail and is one of the central aspects of most static electronic voting systems that are considered sustainable and transparent. See also Rajeev Gore and Vanessa Teague, *Submission 114*, p. 13.

55 C Bennett, 'States ditch electronic voting machines', *The Hill*, 2 November 2014, accessed 6 November 2014, <thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines>.

- 3.75 The move away from electronic voting systems due to these concerns has seen approximately 70 per cent of voters in the 2014 mid-term elections casting a paper ballot.⁵⁶
- 3.76 This departure from electronic voting usage is indicative of the dangers that rapid adoption of electronic voting architecture can bring, especially when maintenance and updating become a second-tier priority after the initial investment. The importance of maintenance, and its cost, is emphasised by Pamela Smith, president of US election watchdog Verified Voting:
- The lack of spending on the machines is a major problem because the electronic equipment wears out quickly. Smith recalled sitting in a meeting with Missouri election officials in 2012 where they complained 25 percent of their equipment had malfunctioned in pre-election testing.
- "You're dealing with voting machines that are more than a decade old," Smith said.
- "There is simply no money to replace them," said Michael Shamos, a computer scientist at Carnegie Mellon University who has examined computerized voting systems in six states.⁵⁷
- 3.77 Interestingly, commentators in the US have not seen the devolution back to paper trails as a negative but rather as a positive:
- The old-school approach seems archaic, but it has an advantage over electronic voting machines: It works.⁵⁸
- 3.78 The march back to the paper-based systems is supported by events such as electronic voting machines in North Carolina and Maryland malfunctioning and automatically flipping votes from Democrat to Republican and vice-versa.⁵⁹

56 K Knibbs, 'Nearly 70 percent of voters this election are casting paper ballots', *Gizmodo*, 4 November 2014, accessed 6 November 2014, <factually.gizmodo.com/nearly-70-percent-of-voters-this-election-are-casting-p-1654239045>.

57 K Knibbs, 'Nearly 70 percent of voters this election are casting paper ballots', *Gizmodo*, 4 November 2014, accessed 6 November 2014, <factually.gizmodo.com/nearly-70-percent-of-voters-this-election-are-casting-p-1654239045>.

58 K Knibbs, 'Nearly 70 percent of voters this election are casting paper ballots', *Gizmodo*, 4 November 2014, accessed 6 November 2014, <factually.gizmodo.com/nearly-70-percent-of-voters-this-election-are-casting-p-1654239045>.

59 P Watson, 'Electronic Voting Machines: Screen Flips Votes in Key US Senate Race', *Global Research*, 4 November 2014, accessed 6 November 2014, <globalresearch.ca/touch-screen-flips-votes-in-key-us-senate-race/5411804>.

3.79 In North Carolina machine malfunctions meant that votes above the winning margin were simply not recorded and as a result were completely lost to the count. It was reported:

An electronic machine in North Carolina lost roughly 4,500 votes in a 2004 statewide race after it simply stopped recording votes.

The race was ultimately decided by fewer than 2,000 votes.⁶⁰

3.80 The US experience serves to highlight the fundamental point that rapid movement to technology-supported voting in reaction to electoral system failures must be tempered with practicality, security and verifiability.

United Kingdom

3.81 The United Kingdom (UK) made a significant investment in electoral modernisation through the use of electronic voting following the 1997 election of the Blair Government. By May 2002 internet, telephone and SMS voting was trialled in local government elections. By the 2003 local government elections, voting by kiosks and digital TV was also trialled.⁶¹

3.82 At the same time as these trials, the UK Electoral Reform Society's Independent Commission on Alternative Voting Methods noted that:

Although increasing numbers of financial transactions are being conducted online, and although many people believe that this means that online voting is safe, the security and privacy issues involved are very different. For instance, financial fraud on the internet is not uncommon, and companies are happy to underwrite this to a certain extent; this is not acceptable in an election. With financial transactions, customers can be issued with a receipt which confirms exactly what happened and when; in order to maintain secrecy and protect the voter from undue pressure, this is not possible with voting. Customers identities' are intrinsically bound to financial transactions; with a vote, the two must (at least to some extent) be separated.⁶²

3.83 Pilot schemes continued for local government elections through to 2007, but the UK Electoral Commission – the independent elections watchdog – found in relation to the 2007 trials that:

60 C. Bennett, 'States ditch electronic voting machines', *The Hill*, 2 November 2014, accessed 17 November 2014, <thehill.com/policy/cybersecurity/222470-states-ditch-electronic-voting-machines>.

61 B Holmes, Parliamentary Library, *e-voting: the promise and the practice*, 15 October 2012, pp. 20-21.

62 Independent Commission on Alternative Voting Methods (UK), January 2002, *Elections in the 21st Century: from paper ballot to e-voting*, accessed 12 November 2014, <electoral-reform.org.uk/downloadfile.php?PublicationFile=3p>.

the level of implementation and security risk involved was significant and unacceptable. There remain issues with the security and transparency of the solutions and the capacity of local authorities to maintain control over the elections.⁶³

- 3.84 No information is available from the UK Electoral Commission on why electronic voting trials have not been continued, and the Australian Parliamentary Library notes:

the online voting initiatives withered for reasons that are not at all clear. There were no published outcomes from the consultation paper [on electronic democracy issued by the Leader of the House of Commons]. The dedicated website 'edemocracy.gov.au' eventually disappeared.⁶⁴

- 3.85 The only voting options now available to UK voters are in person at a polling station, by post or by proxy.⁶⁵

Other jurisdictions

- 3.86 Various methods of electronic voting are in use in other jurisdictions, either in the form of static electronic voting or some elements of internet voting.
- 3.87 The majority of internet voting is restricted to trials, pilots or smaller municipal election exercises. Many countries have trialled internet voting, and these trials are either continuing or have been discontinued.
- 3.88 India has had wide-ranging use of portable electronic voting machines (EVMs) since 2004. The portable machines are used in polling places to allow voters to press a button on a ballot unit that is connected to a control unit that is capable of recording a limited number of votes, which are then downloaded and tallied electronically.⁶⁶
- 3.89 Despite the simplicity and 'hard-wired' nature of the EVMs used in India, there have been many reported attempts and successes in hacking and manipulation of ballot data.⁶⁷

63 The Electoral Commission (UK), *Key issues and conclusions: May 2007 electoral pilot schemes*, August 2007, accessed 12 November, <http://electoralcommission.org.uk/_data/assets/electoral_commission_pdf_file/0015/13218/Key_findingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf> 2014.

64 B Holmes, Parliamentary Library, *e-voting: the promise and the practice*, 15 October 2012, p. 22.

65 The Electoral Commission (UK), *How to Vote*, accessed 12 November 2014, <<http://www.electoralcommission.org.uk/i-am-a/voter/how-to-vote>>.

66 Election Commission of India, *EVM*, accessed 20 August 2014, <http://eci.nic.in/eci_main1/evm1.aspx>.

67 *Bhatkallys*, undated, 'US scientists 'hack' India electronic voting machines,, accessed 20 August 2014, <bhatkallys.com/ىوىىند/us-scientists-hack-india-electronic-voting-machines/>.

- 3.90 This system is also suitable for, and supported by, the single-vote first-past-the-post system of voting in the Indian lower house (Lok Sabha). It is also now supplemented by the fact that, since late 2013, Indian voters have had a 'none of the above' voting option on the EVMs.⁶⁸
- 3.91 New Zealand and Canada, two countries which share Australia's Westminster-style political system, have been conservative with regard to electronic voting and have largely confined their interest in the topic to discussions.
- 3.92 Switzerland has been trialling internet voting since 1998. Until now, these trials have been restricted to referenda in selected cantons within Switzerland.⁶⁹ Nationally, the Swiss government plans to allow Swiss expatriates to vote online in the next parliamentary elections in October 2015, with plans to expand to the greater population in the future.⁷⁰

68 *BBC News*, 27 September 2013, 'India voters get right to reject election candidates', accessed 1 September 2014, <bbc.com/news/world-asia-india-24294995>.

69 R Smith, July 2009, *International Experiences of Electronic Voting and Their Implications for New South Wales*, NSWEC, Sydney, accessed 13 November 2014, <elections.nsw.gov.au/__data/assets/pdf_file/0013/103207/International_Experiences_of_Electronic_Voting_and_Their_Implications_for_New_South_Wales_Report_2009.pdf>, pp. 12-13.

70 S Fenazzi, 'Direct democracy enters new phase of digital era', *SWI*, 15 August 2013, accessed 7 November 2014, <swissinfo.ch/eng/direct-democracy-enters-new-phase-of-digital-era/36655004>.

- 3.93 Despite the Swiss government's confidence in developed systems, there have been reports of successful manipulation of digital votes by virus implantation,⁷¹ and security analysis has established the physical and data integrity concerns typical to systems as they are developed and implemented.⁷²
- 3.94 In 2013, Norway trialled internet voting, however, has ended trials because of security concerns and a lack of evidence that the trials led to increased participation. There was also evidence that a small percentage of people voted twice – once on the internet and then at a polling booth.⁷³
- 3.95 It is also worth noting that the majority of countries that allow for wider-scale electronic voting (including some of those outlined here) have some form of national identity card or identifier, which allows for individual verification of a voter's identity, either photographically in a polling booth or via a unique identifier when remote polling occurs (as with Estonian remote voting).
- 3.96 Some countries with identifiers (such as The Netherlands) have nonetheless determined that the risks of electronic voting outweigh the benefits.

Committee comment

- 3.97 Advocates of electronic voting point to international use to support the case that its use is becoming widespread, ignoring the strong evidence of security and cost concerns and moves to return to the provision of paper-based voting options.
- 3.98 It is difficult to undertake a comparative study of the systems used in international jurisdictions and their applicability to the Australian electoral context due to the significant differences in electoral systems.
- 3.99 For example, advocates cite Brazil and India's use of voting machines, without recognising the specific issues the use of these machines address

71 S Fenazzi, 'Direct democracy enters new phase of digital era', *SWI*, 15 August 2013, accessed 7 November 2014, <swissinfo.ch/eng/direct-democracy-enters-new-phase-of-digital-era/36655004>.

72 A Baumann and D Häberli, University of Fribourg (Switzerland), 1 December 2013, *A Security Analysis of the Swiss Electronic Voting System*, accessed 7 November 2014, <diuf.unifr.ch/main/is/student-projects/thesis/security-analysis-swiss-electronic-voting-system>.

73 *BBC technology News*, 27 June 2014, 'E-voting experiments end in Norway amid security fears', accessed 12 November 2014, <bbc.com/news/technology-28055678>.

such as low literacy levels and the thousands of candidates that run in each election.

- 3.100 Advocates also cite current Estonian and Swiss internet voting as improving equality and voter turnout, convenience and timely vote counting. However, these examples have either been consistently undermined in security analyses (in the case of Estonia) or have not been proven in a general election (in the case of Switzerland).
- 3.101 This advocacy does not take into consideration relevant features of Australia's electoral system such as compulsory voting, which provides some inherent assurances for voter equality, or the complex counting for the Senate single-transferrable-vote (jurisdictions with the most widespread static voting machines have a first-past-the-post system).
- 3.102 Advocates also do not effectively argue the need for a more timely determination of results. Most House of Representatives seats are determined on election night, and for those seats which are close, ensuring count accuracy is far more important than ensuring timeliness.
- 3.103 Further, the Committee is not convinced that convenience should be privileged above other legitimate aspects of the electoral process. Voting is the most important civic duty that all citizens must undertake. There is a need to ensure that this is not undermined for the sake of convenience.
- 3.104 The future use of technology for elections in the Australian context is explored further in Chapter 4.

The use of technology in Australian elections

- 4.1 Electronic voting is considered by many to be a necessary, or at least the most logical, next step in ensuring the ongoing accessibility of the electoral process to all Australians.
- 4.2 In particular, electronic voting can be seen as providing an empowering alternative for those who find that more traditional methods of voting are inadequate or pose access, secrecy or time constraints, such as blind or low vision voters, those with mobility or access issues, culturally or linguistically diverse citizens and internationally deployed Defence or Antarctic service personnel.
- 4.3 As noted in Chapter 1, commentary in the wake of the lost ballots in Western Australia (WA) called for an immediate move to electronic voting, specifically the ability to vote online.
- 4.4 Electronic voting, particularly in relation to internet voting, raises a number of complexities and concerns. One real concern is maintaining a secret ballot free of coercion – a foundation principle of Australian democracy since its first use in Victoria in 1856, and a central element of every federal election since 1901.¹
- 4.5 The Australian Government Information Management Office notes that:

Representative democracy depends on large numbers of people electing small numbers of people to exercise powers that the constitution accords to elected representatives. Voting needs to be conducted in a context free of undue influence, or at least of

1 Australian Electoral Commission (AEC), *Australia's major electoral developments timeline: 1788-1900*, accessed 6 November 2014, <aec.gov.au/Elections/Australian_Electoral_History/reform.htm>.

coercion and a climate of fear. Voting systems must therefore be designed to protect every voter's choices against disclosure. The integrity of a voting system is also critical to public confidence. It must resist manipulation, and ensure that the vote count reflects the votes actually cast. The system's security and integrity must be both demonstrated in advance, and audited in arrears. Achieving these objectives is very challenging.²

- 4.6 The comprehensive introduction of electronic voting would constitute a 'fundamental reshaping of Australia's electoral processes'.³ While many consider a shift to electronic voting to be inevitable, it is crucial that questions are asked about the impact such moves will have on our democratic system.
- 4.7 This chapter explores the arguments in support of proposals to introduce electronic voting and the costs, safety and desirability of these proposals.

Arguments in support of electronic voting

- 4.8 The three main perceived benefits of introducing universal electronic voting in Australia relate to:
- providing a secret ballot for blind and low vision voters;
 - more easily delivering remote voting services; and
 - securely handling ballots.

Blind and low vision voters

- 4.9 At present, blind or low vision voters have an option of voting via the assisted telephone voting system as outlined in Chapter 3.
- 4.10 Despite commending the Australian Electoral Commission (AEC) for its delivery of this option, Vision Australia argued that many potential users have chosen not to use this system because:
- although anonymous, the vote is not secret;
 - below the line Senate voting was extremely difficult to do over the phone;
 - the call centre implies a lack of independence by the reliance on a third party; and

2 Australian Government Information Management Office, *Future Challenges for E-Government*, p. 49, accessed 15 August 2014, <finance.gov.au/publications/future-challenges-for-egovernment/docs/AGIMO-FC-no3_.pdf>.

3 Tom Rogers, a/g Electoral Commissioner, *Transcript of Evidence*, 31 July 2014, Canberra, p. 2.

- there is no way to verify that voting intention has been lodged correctly.⁴
- 4.11 Vision Australia and Blind Citizens Australia argued for an electronic voting system that is ‘100 per cent secret, independent and verifiable’.⁵
- 4.12 Both organisations commended the New South Wales (NSW) Electoral Commission for providing the iVote system (also discussed in Chapter 3), and recommended its use in federal elections.
- 4.13 Blind Citizens Australia further argued that electronic voting options should be extended to all voters with a disability due to the difficulty faced by some in attending an accessible polling place.⁶
- 4.14 Vision Australia also argued that providing a more accessible voting option at polling places for those who are blind or who have low vision would provide greater engagement in the electoral system:
- Some clients also reported that they took their children to the polling centre on the 2013 election day so that the family as a whole could discuss the election process and how it was conducted, and also so that their children could learn that having a disability does not preclude community participation. People who are blind or have low vision must have the option to engage with the rest of the community in shared activities. It is therefore important that some voting options are made available at polling places on election day even if accessible options are provided that allow people to cast pre-poll votes and to vote from home. Equally, we feel that partners and spouses of voters who are blind or have low vision should be able to take up an accessible voting option so that family cohesion and activity is maintained.⁷
- 4.15 The extension of a secret, voter-verifiable voting option to people who are blind or who have low vision is one of the most compelling arguments for the introduction of limited electronic voting. No person should be disenfranchised because of a disability, and the Australian Government also has an obligation to make the electoral system as accessible as possible to ensure a secret ballot.
- 4.16 This obligation not only relates to equal access and democratic participation on a domestic level, but also relates to blind or low vision voters exercising their internationally codified right to equal access to

4 Vision Australia, *Submission 141*, pp. 6-7.

5 Blind Citizens Australia, *Submission 97*, p. [3]. Michael Simpson, General Manager Accessible Information, Vision Australia, *Transcript of Evidence*, 15 April 2014, Melbourne, p. 48.

6 Blind Citizens Australia, *Submission 97*, p. [6].

7 Vision Australia, *Submission 141*, p. 10.

democratic procedure and a secret vote as outlined in Article 29 of the United Nations Convention on the Rights of Persons with Disabilities.⁸

Remote voting services

- 4.17 A particular issue faced by Australian electoral officials in all jurisdictions is the vast geographical spread of the population and the associated challenges that come with staffing and equipping remote locations.
- 4.18 Given the existing circumstances of voting in places like Antarctica which already have an inherent risk to the secrecy and security of the ballot, there is, therefore, an argument for the limited provision of electronic voting in these circumstances to improve access to voting. That is, the relative risk would not be increased though a limited provision of electronic voting given the existing circumstances.

Logistics

- 4.19 Bodies involved in the electoral process have reported difficulties in providing and receiving voting and ballot materials overseas due to transit delays and tight legislative timelines. This has the potential to become even more difficult as postal services decrease.⁹
- 4.20 In addition to better geographic coverage, internet voting also potentially provides significant scope for cost savings because it allows global reach with very little permanent infrastructure outlay or logistical overheads. There are no shipment or postal costs, and also no delays in sending or receiving voting material.
- 4.21 Australia Post submitted in support of electronic voting noting that internet voting could negate:
- time lags due to physical delivery of postal votes;
 - unnecessary costs associated with the higher number of applications versus actual postal voters;
 - delays in knowing the result of an election due to the counting of postal votes; and
 - concerns over the integrity of the vote where there might be concerns that some voters have voted under the influence of others.¹⁰
- 4.22 Despite the availability of postal voting, the AEC also commits significant resources to the provision of mobile polling teams for both urban and
-

8 United Nations Convention on the Rights of Persons with Disabilities, accessed 4 September 2014, <un.org/disabilities/convention/conventionfull.shtml>.

9 Ahmed Fahour, Managing Director, Australia Post, Speech, *Australia Post at a turning point*, 14 August 2014, accessed 7 September 2014, <auspost.com.au/about-us/aicc-speech.html>.

10 Australia Post, *Submission 174*, p. 12.

- remote locations.¹¹ This is a significant cost that advocates point out could be ameliorated if internet voting were implemented.
- 4.23 It is further argued that internet voting also has the potential for savings through reductions in the duration of temporary employment of election officials and reduced costs in the production and distribution of ballot papers – particularly to overseas posts and deployed Defence personnel. Arguably, the unit cost of each vote cast via internet voting is likely to be substantially lower than the unit cost of ordinary or postal votes (which includes postage, printing and preliminary scrutiny costs).¹²
- 4.24 While internet voting has the potential to offer these cost savings, this does not make internet voting desirable when considering the security and sanctity of the ballot, as discussed further below.
- 4.25 Some participants in the inquiry suggested using third party or other Australian Government providers in order to utilise existing electronic networks and identity mechanisms.¹³ While utilising existing networks could provide efficiencies or potential savings, the underlying but crucial issue of trust in the system would likely be put at risk if voting was entrusted to entities not subject to the accountability requirements of the Electoral Act.
- 4.26 It is unlikely that internet voting would completely negate the need to provide a paper ballot option, which could mean an effective doubling of service provision. It is also doubtful that internet voting would negate the need for the AEC to have a presence in remote areas.

Secure handling of ballots

- 4.27 It has been widely argued in the media and throughout this inquiry that electronic voting has the potential to mitigate the failings that led to the events that occurred in WA during the 2013 federal election. One argument advanced was that a ‘large scale paper voting system is inherently insecure’:

Many links in the paper vote processing chain, including movement and storage of ballots, rely on the integrity and competence of tiny groups of people – sometimes just one person.¹⁴

11 AEC, *Submission 20.3*, p. 54.

12 Electoral Council of Australia and New Zealand (ECANZ), *Internet voting in Australian election systems*, 10 September 2013, p. 18.

13 Australia Post, *Submission 174* and Department of Communications, *Submission 118*.

14 Big Pulse, *Submission 178*, pp. [1-2]. See also Cathy McGowan MP, *Submission 167*, Clive Palmer MP, *Submission 92*.

- 4.28 However, the argument that the lost WA ballot papers are a reason to move to electronic voting does not appear to be supported by evidence that the inherent vulnerabilities of a paper-based voting system are any greater than those of an electronic system.
- 4.29 Indeed, evidence to the inquiry indicates a similar ‘lost votes’ error rate with an electronic system without the advantage of a verifiable paper trail for remaining votes:
- Paper processes are not perfectly secure or reliable, but neither are computers. For example, the lost vote rate in the 2013 West Australian Senate race (1370 out of 1,348,797, slightly over 0.1%) was about the same as the demonstrated vote misrecording rate in Australia’s largest Internet voting trial, the NSW iVote project (43 misrecorded electronic votes out of 46,864, slightly under 0.1%) (PWC, 2011). The WA Senate incident received much more attention because it impacted an election outcome, not because the system was inherently much less reliable. Even more importantly, the paper-based Senate process retained paper evidence of the 99.9% of votes that weren’t lost; the iVote system produced no meaningful evidence of the correctness of any of the votes. Reliability, privacy and verifiability must be designed into electronic voting processes as carefully as they are designed into our existing paper-based processes.¹⁵
- 4.30 Further, the ‘weak point’ in a paper-based voting system, resulting in a lost box of ballot papers, may lead to an unverifiable close result (such as in WA): but one ‘weak point’ in a wide-ranging electronic voting system has the potential to expose an entire election’s vote data to manipulation, corruption or attack, undermining the parliamentary system supported by the electoral process.¹⁶
- 4.31 Nonetheless, certain elements of electronic support for voting, in particular the digitisation and capture of ballot papers, have the potential to provide a solution to the events that occurred during the 2013 federal election.

15 Rajeev Goré and Vanessa Teague, *Submission 114*, pp. 6-7.

16 L Tung, ‘10 ways e-voting could save or destroy democracy’, *The Sydney Morning Herald*, 25 April 2014, accessed 4 September 2014, <smh.com.au/it-pro/government-it/10-ways-evoting-could-save-or-destroy-democracy-20140425-zqxni.html>.

Safety, cost and desirability

- 4.32 The main concerns with electronic voting relate to:
- safety, including the security, integrity and transparency of the system;
 - cost of delivering a safe system;
 - desirability of electronic voting, including:
 - ⇒ the capacity to maintain the secrecy of the vote; and
 - ⇒ the effect on voter behaviour and confidence in the electoral system.

Safety of electronic voting

- 4.33 The safety of electronic voting systems is often simplified into the physical security of a voter, the vote cast and the safeguards attached to data transmission or storage of the vote once cast.
- 4.34 However, there are more complex interconnections between the security of electronic voting (as evidenced in the criticisms of international systems in Chapter 3), the integrity that a voter perceives in the system in which they are voting (both through tangible security measures and the psychological value that a voter places on the method used to cast their vote), and the transparency and visibility that must accompany any voting system, to ensure that all stakeholders can believe the veracity of the outcome.
- 4.35 Ultimately, the voter's perception of the voting process as a whole, and their acceptance of the process as 'safe', will dictate the success of any electoral system and the confidence voters have in the resultant government. The question that remains is: is this safety undermined in the current Australian system and can it be addressed wholly and satisfactorily by electronic voting, or will electronic voting introduce new and greater safety concerns?

Security and integrity

- 4.36 Public confidence in the security and integrity of any voting system is integral to ensuring confidence in election outcomes. The international examples outlined earlier in this report highlight the fact that, even though the technology currently exists to provide for electronic voting, the integrity and security of such systems can be vulnerable. In the case of Estonia's remote internet voting system, an independent analysis recommended discontinuation of the system due to fundamental security and data integrity flaws.

4.37 Proponents of electronic voting have cited the widespread use of secure online banking. But these systems, along with government systems, are not impervious to attack:

Electronic security breaches on important government and financial infrastructure are common. For example, last month an attack on a government website in the US state of Oregon caused “elections and business databases to go offline”. The attack was described as “an orchestrated intrusion from a foreign entity” (Zheng, 2014). In 2012 a sophisticated Trojan stole € 36 million from European Internet banking systems (Kalige & Burkey, 2012). Even more concerning are stories of systematic compromise of Internet sites and infrastructure by the Chinese People’s Liberation Army (Mandiant, 2013) and the US NSA. Last week it was revealed that half a billion dollars’ worth of bitcoins had been stolen from one of the world’s largest bitcoin exchanges (Sydney Morning Herald, 2014). Electronic voting systems would not be immune from such attacks. Indeed, Internet voting is harder to secure (for privacy reasons) and has higher stakes than most other Internet applications (Jefferson).¹⁷

4.38 This supports the argument that even if internet voting was completely secure at a given point in time, this would be no guarantee of future security as it is difficult to anticipate the future capability of those wishing to mount attacks.

4.39 Internet voting is considered by experts to be the most risky and difficult mode of electronic voting to implement. Even if it were to be demonstrated that voting over the internet could remain secret, in the future there is no guarantee that, given the pace of technological advancement, a person’s past voting record could not be observed. With paper ballots the secrecy of the vote is guaranteed on polling day and forever thereafter.

4.40 Professor Rajeev Goré, of the Research School of Computer Science at the Australian National University was blunt in his assessment:

First of all ... internet voting is just too dangerous. Don't do it. It is as simple as that.¹⁸

4.41 It is important to recognise the distinctiveness of voting as compared to other activities, transactions or services conducted over the internet. Almost every information and communication technology (ICT) application is built in a way that allows for verification of its proper

17 Rajeev Goré and Vanessa Teague, *Submission 114*, p. 5.

18 R Goré, *Transcript of Evidence*, 26 March 2014, Canberra, p. 2.

functioning by observing the application's outputs.¹⁹ This verification process is crucial to gaining user confidence in the system. For example, online banking allows the user to log in, see up-to-date information relating to their account and monitor their transactions.

4.42 This type of verification process presents a problem for internet voting, because our democratic system seeks to maintain the individual's right to the secrecy of their vote. This means separating the identity of the voter from the vote cast, which inevitably makes verification – the hallmark of all other trusted ICT technologies – difficult. Breaking the link between voter and vote means that the examination of an internet voting system after an election cannot prove directly that every vote was indeed counted and tallied as cast.²⁰

4.43 In relation to isolated static electronic voting, the Australian Capital Territory (ACT) electronic voting system is an example of how physical security can be maintained by isolating terminals and ensuring they have no connection to any other network, therefore reducing the avenues for compromising data. The ACT Electoral Commissioner outlined the security basis for the ACT system:

we have decided to ... opt for something that is entirely self-contained and entirely wired within the polling place. So it uses a computer that is a server in the polling place that is in a locked cabinet. The voting clients are all connected by ethernet cables, and one of the conscious decisions we made was to make it very difficult to be able to remotely get into the system. So you would have to actually physically get into the server in a locked box in a locked polling place in order to have any means of getting into the system itself.²¹

4.44 This form of physical security isolation is a strong attempt at controlling potential manipulation, but many people have access to the machines at different stages during an election, so the opportunity for the manipulation of machinery, firmware or software still exists.²² This security is also dependent on the provision of physical voting terminals, which would be a cost-prohibitive method of introducing electronic voting

19 International Institute for Democracy and Electoral Assistance (International IDEA), December 2011, *Introducing Electronic Voting: Essential Considerations*, p. 6, accessed 20 May 2014, <idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>.

20 International IDEA, December 2011, *Introducing Electronic Voting: Essential Considerations*, p. 7, accessed 20 May 2014, <idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>.

21 Phillip Green, ACT Electoral Commissioner, *Transcript of Evidence*, 29 July 2014, Canberra, p. 2.

22 Rajeev Goré and Vanessa Teague, *Submission 114*, p. 12.

across Australia for federal elections. Even in a jurisdiction as small as the ACT, universal implementation of electronic voting is constrained by the cost of providing access at every polling booth.

- 4.45 One response to potential issues with integrity and security in relation to isolated static electronic voting is to introduce accompanying paper trails. The systems most commonly used internationally rely on paper trails to mitigate public distrust and verification problems.
- 4.46 As noted in Chapter 3, in 2002, for example, United States (US) electoral authorities made a large investment in e-voting machines.²³ This became problematic, however, due to the rapid adoption of electronic-only systems that lacked any manual verification, and by 2008 many states required paper trails to ensure the veracity of votes cast and greater transparency in the system, with the result that many of the machines originally purchased were rendered obsolete. As of 2010, 40 states had moved towards requiring paper trails.²⁴
- 4.47 The introduction of paper trails makes systems more complex and expensive, which is not ideal. In addition, implementing paper trails to facilitate the building and maintenance of trust in the system (for example with proper audit processes and mandatory random sample recounts) could be said to somewhat defeat the purpose of moving away from paper ballots.

Transparency

- 4.48 Any electronic voting system must be fully open to scrutiny to ensure confidence that votes are being recorded and tallied correctly. With a paper ballot system, all handling of ballot papers from printing to final storage can be observed. This becomes more difficult with an electronic system because a person cannot easily observe the computer's processes.
- 4.49 Permitting public scrutiny of software source code is one way of ensuring transparency in an electronic voting system:
- Computerised voting systems, including their source code, all documentation and reports, and the associated physical security procedures should be available to e-voting and security experts and the public. Source code availability should be enhanced by enough support for compiling, running and understanding the

23 This was predominantly in reaction to the controversy surrounding the 2000 presidential election and was facilitated by the federal *Help America Vote Act* (2002).

24 International IDEA, December 2011, *Introducing Electronic Voting: Essential Considerations*, p. 25, accessed 20 May 2014, <idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>.

system. This level of transparency should be an enforced condition of the initial tender and contract ...

Having the open source available to the community for technical review by a range of interested experts will increase transparency and trustworthiness of the electronic voting and counting process, because it facilitates an open and scientifically informed discussion about the merits of a proposed system.²⁵

- 4.50 While such access to source code may enable expert review and discussion, it would also open a system to scrutiny by entities with malicious intent, requiring a balance to be struck between security and transparency.
- 4.51 Ownership of the technology or intellectual property is also relevant here. It may only be possible to ensure public access and scrutiny if the technology or intellectual property is not owned by a private corporation that has an interest in protecting proprietary software. There is also the potential for commercial or political influence on a supplier to undermine transparency and accountability. In terms of electronic voting in Australia, these types of factors would suggest the desirability of the AEC developing its own system.

Cost of electronic voting systems

- 4.52 An important factor to consider in the delivery of elections is whether the cost and cost-effectiveness of electronic voting is a significant barrier to its implementation.
- 4.53 Quantifying the potential cost of electronic voting in the Australian context is very difficult, given the limited history of electronic voting delivery at a federal level in the past. Using a 'cost per vote' measure, the current trials of electronic voting at a federal level are not cost-effective.
- 4.54 As outlined in Chapter 3, the 2007 trials of electronic voting for deployed Australian Defence Force (ADF) personnel and voters with Blind or Low Vision had considerable costs attached:
- \$1 159 per vote for ADF votes; and
 - \$2 597 per vote for Blind or Low Vision votes.²⁶
- 4.55 The total cost of the 2013 election, excluding the WA re-run Senate election and the cost of public funding, was \$132 906 303.²⁷ Based on the House of

25 Rajeev Goré and Vanessa Teague, *Submission 114*, p. 5.

26 Joint Standing Committee on Electoral Matters, March 2009, *Report on the 2007 federal election electronic voting trials*, pp. 25, 50.

27 AEC, *Submission 20.3*, p. 131.

Representatives voter turnout of 13 726 070,²⁸ this equates to roughly \$9.68 per vote.

- 4.56 Universal implementation of static electronic voting is simply not cost effective. Even where an investment has been made in static voting, scalability does not reduce costs. Despite the small electoral area within the ACT, the deployment of electronic voting to all polling places is not proposed simply due to costs:
- the deployment of the required hardware to polling places for a single day poses logistical challenges and is of questionable cost effectiveness.²⁹
- 4.57 As discussed in Chapter 3, the development of the universal static electronic voting system in Ireland cost over €54 million (approximately A\$78 million). The up-front purchase of the machines is not the only cost, but the total cost of ownership, including review, software upgrade, maintenance and replacement is significant. These ongoing costs contributed to Ireland abandoning electronic voting.³⁰
- 4.58 Other electronically-assisted voting (non-static) is more cost-effective. The NSW iVote system (outlined in Chapter 3) used in the 2011 state election had an average cost per vote cast of \$74 compared to an average cost of all votes cast of \$8. This cost per vote reduces significantly as the system is scaled up to 200 000 voters using the system, with an estimated average cost per vote being approximately \$24.³¹
- 4.59 The capacity to utilise this system in local government elections also further reduces the cost and is considerably more cost effective for delivery of services to blind and low vision voters than previous methods used (braille ballot papers).³²
- 4.60 Nonetheless, there are questions about the security of the NSW iVote system and the capacity for its use in federal elections. In addition, the

28 AEC, results 2013 federal election, House of Representatives turnout by state, accessed 31 October 2014, <results.aec.gov.au/17496/Website/HouseTurnoutByState-17496.htm>.

29 ACT Electoral Commission, June 2005, *Electronic voting and counting system: review 2004*, p.4, accessed 14 July 2014, <elections.act.gov.au/__data/assets/pdf_file/0006/1797/2004electionreviewcomputervoting.pdf>.

30 Department of Environment, Community and Local Government (Ireland), Media Release, *Minister Gormley announces Government decision to end electronic voting and counting project*, 23 April 2009, accessed 3 October 2014, <environ.ie/en/LocalGovernment/Voting/News/MainBody,20056,en.htm>.

31 Allen Consulting Group, *Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011*, 11 July 2011, pp. 40-44.

32 Allen Consulting Group, 11 July 2011, *Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011*, p. 44.

experience in international jurisdictions outlined in the previous chapter also makes clear that any electronic system needs to have an associated verifiable paper trail. This not only duplicates the voting process, but increases the cost of electronic voting systems to the point that they are not cost-effective.³³

Desirability of electronic voting systems

Secrecy of the vote

4.61 A significant concern in relation to electronic voting is the manner in which such technology may undermine the secret ballot, particularly in relation to internet voting.

4.62 The Australian Constitution requires that both houses of Parliament be elected 'directly chosen by the people' and the secrecy of the ballot was enshrined in the first Electoral Act of 1902, and remains in section 233 of the *Commonwealth Electoral Act 1918*.

4.63 In addition, the secret ballot is a fundamental principle of a democratic society that is enshrined in the Universal Declaration on Human Rights (Article 21(3)):

The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.³⁴

4.64 This right, and the protection of it, also underpins electoral administration bodies such as the AEC:

Traditionally, the one real role of an electoral administration body like the AEC is to provide a safe, secure place where individuals can go and cast a vote without anyone looking over their shoulder or coercing them in casting that vote.³⁵

4.65 Internet voting removes the guarantee of a secret ballot, exposing voters to a greater risk of influence. This influence may not be malicious (it may be family based, for example a grandchild voting on behalf of a grandparent uncomfortable with technology and affecting their voting intentions), but nonetheless, it diminishes the secrecy of the ballot:

33 International IDEA, December 2011, *Introducing electronic voting: essential considerations*, p. 18, accessed 20 May 2014, <idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>.

34 The *Universal Declaration of Human Rights*, viewable at <un.org/en/documents/udhr/index.shtml#a21>

35 Tom Rogers, a/g Electoral Commissioner, *Transcript of Evidence*, 31 July 2014, Canberra, pp. 12-13.

The argument basically is that people value their civic role, their civic duty. That is very important for people and they take it very seriously. When they are voting in a public place they will honour their civic duty and they will vote according to their true preference. However, the reality is that for a very large proportion of the population their civic duty comes second to their familial duty, their duty to their family. If they have to choose, they will put their duty as a spouse, a father, a son, a mother or a daughter above their civic duty. That is not something on which I particularly have a view. I see it as a reality. I think it is unrealistic to expect people to put their civic duty above their duty within the family.³⁶

- 4.66 In some US states that allow internet voting for members of the armed forces deployed overseas, the risk of compromise to the secret ballot is so high that:

some of the 30 or so states that allow Internet voting for service members now require them to sign a form saying they understand that by using the system, their ballot may not be secret.³⁷

- 4.67 The State of Alaska warns voters returning their ballot through its 'Secure Online Voting Solution' that:

When returning the ballot through the secure online voting solution, your [sic] are voluntarily waving [sic] your right to a secret ballot and are assuming the risk that a faulty transmission may occur.³⁸

- 4.68 In addition, as noted in Chapter 3 and above, online voting systems have been found to be the most risky and vulnerable, raising questions about the secrecy and veracity of the vote. Indeed, it has been reported in the US that:

The National Institute of Standards and Technology, at the direction of Congress, has conducted extensive research into Internet voting in the last decade and published several reports that outline all the ways votes sent over the Internet can be manipulated without detection. After warning that there are many possible attacks that could have an undiscovered large-scale

36 Prof Sarah Birch, *Private Briefing*, 29 July 2014, Canberra.

37 E Weise, 'Internet voting not ready for prime time', *USA Today*, 3 November 2014, accessed 6 November 2014, <usatoday.com/story/tech/2014/11/02/internet-voting-not-secure/18269285/>.

38 State of Alaska, Division of Elections, *Absentee voting by electronic transmission*, accessed 6 November 2014, <elections.alaska.gov/vi_bb_by_fax.php>.

impact, the institute concluded that secure Internet voting is not yet achievable.³⁹

- 4.69 The only way to guarantee a secret electronic vote is through the use of isolated static electronic voting machines. These have massive upfront and ongoing maintenance costs and evidence from international jurisdictions, particularly the US, indicates that they need to be accompanied with a verifiable paper trail – something which somewhat defeats the purpose by merely replacing pencils with touchscreens or buttons.

Effect on voting culture, voter behaviour and confidence in the electoral system

Voting culture and voter behaviour

- 4.70 Proponents of expanding electronic voting options can underestimate the value that many members of society place on the act of voting and the historical significance that this democratic process embodies.
- 4.71 The Parliamentary Library has captured this concept well:
- In representative democracies, voting for members of legislatures is a foundational activity, and the methods, traditions and dynamics that characterise that voting act are usually a distinctive – and often cherished – element of the political culture that exists in the country or jurisdiction concerned.⁴⁰
- 4.72 The 2001 joint report of the AEC and the Victorian Electoral Commission on electronic voting identified issues relating to electronic voting that extend beyond its technological merits:
- The technical barriers to wide spread implementation of e-voting are considerable. There are also the democratic issues of secrecy of the elector's vote, equal access to e-voting by voters and public confidence in the system.⁴¹
- 4.73 The AEC has previously noted the importance of garnering public support and maintaining the strong voting culture in Australia in relation to introducing electronic voting:
- There is no evidence to suggest that there is any political or community support for changing the voting systems presently used in Australia. This is an important point to appreciate when

39 B Simons, 'Online voting rife with hazards', *USA Today*, 4 November 2014, accessed 12 November 2014, <usatoday.com/story/opinion/2014/11/04/barbara-simons-online-voting-problems/18461679/>.

40 B Holmes, Parliamentary Library, *e-voting: the promise and the practice*, 15 October 2012, p. 1.

41 Victorian Electoral Commission, September 2002, *eVolution no revolution: Electronic voting status report 2*, p. 19, accessed 13 November 2014, <vec.vic.gov.au/files/RP-EvolutionNotRevolution.pdf>.

considering the possibility of introducing any form of electronic voting in this country. In our view, the introduction of any form of electronic voting must support the present voting systems and voting culture.⁴²

4.74 While the voting culture using paper ballots in polling booths is strong in Australia, the events of the 2013 election have affected this support, and, as noted above, electronic voting has been suggested as a solution. Electronic voting is also considered by many to be the next step in ensuring the ongoing accessibility of the electoral process.

4.75 There is emerging research which suggests that electronic voting may have a detrimental effect on voting behaviour.⁴³ Research also indicates that the element of ritual involved in the act of voting at a public polling place plays a role in sustaining people's sense of shared civic engagement and confidence in their democracy. In this context, a shift to electronic voting may downgrade the social significance of voting:

Not only will e-voting fail to reverse electoral apathy, it will actually lead us in the wrong direction. Voting is more than the simple act of indicating one's political preference. It's a vital public ritual that increases social solidarity and binds citizens together. ... So, if everybody will be able to e-vote, and if e-voting is essentially fraudproof, what could be wrong with it? The problem is that e-voting will transform voting, an inherently public activity, into a private one. Even with the secret ballot, the mechanics of voting are still explicitly designed to remind us that, in principle, we are all equal members of a political community. On Election Day, we must leave our homes and offices, travel to a polling place, and physically mingle with people who are plainly our equals that day, no matter what other differences we have. Voting, as we currently do it, is a civic ritual, however brief it may be.

This ritual is valuable not just because it makes us feel good about ourselves. It also gets us to think about public issues differently than we would do otherwise. While it's generally assumed that people vote on the basis of their pocketbooks, surveys show that most people actually focus on things such as the national good, not their narrow self-interests, when they vote. One possible reason

42 AEC, March 2001, *Electronic voting and electronic counting of votes*, accessed 13 November 2014, <aec.gov.au/Voting/report.htm>.

43 S Birch. 'The Social Dimension of Electronic Voting: How the Use of Technology in the Voting Process Can Alter the Meaning of Elections', p. 3 *Presentation to the Annual Conference Association of European Electoral Officials*, London, 23-25 October 2003, accessed 13 November 2014, <aceeeo.org/images/file/London%20Conference/sarah_birch.pdf>.

for this: when people are obliged to leave their homes and enter the public sphere, as they do when the vote, they tend to become more public minded.

E-voting, then, might aptly be called “voting alone”. If our era is a time of citizen disengagement, of staring at screens and passing in and out of our gated communities or apartment fortresses as we wave to private security personnel, then e-voting from home is all too congruent with the spirit of the age. Far from enriching democracy, e-voting pushes us towards political anomie.⁴⁴

- 4.76 Professor Graeme Orr of the University of Queensland also cautioned against the widespread adoption of electronic voting because of the wider democratic participation opportunities that election day affords:

Electronic voting, I hope, is not on the cards for reasons of cost, practicality, equity and ritual. Internet voting is hackable and would require a ‘reinvent the wheel’ paper trail. Computerised voting at polling stations would involve a very large outlay; be less fail-safe than paper ballots in some ways, given how our elections depend on thousands of part-time citizen employees; and computerised voting and polling stations may be impossible to deliver equally in many rural areas. In any event, paper ballots allow genuine and meaningful participation by thousands of citizens as scrutineers. It also lets those who want to protest in a compulsory system to scribble on the ballot as a form of participation, which is important.⁴⁵

Confidence in the electoral system

- 4.77 As the 2013 election has highlighted, when errors occur in the voting system, it undermines public confidence not only in the electoral process, but in election outcomes. Errors, problems or irregularities in an electoral process will always have the effect of undermining public confidence, whether the voting system is paper-based or electronic:

But I think the underlying issue with both of those is that when something goes wrong with any type of voting system – it does not have to be electronic voting – it undermines confidence in the electoral process. It can take a very long time for confidence to recover. We saw this in Florida, in the United States, after the 2000 elections where surveys showed that people still had perceptions

44 R Valelly, ‘Voting Alone: The case against virtual ballot boxes’, *The New Republic*, 13 & 20 September 1999, quoted in ECANZ, *Internet voting in Australian Electoral Systems*, 10 September 2013, pp. 63-64.

45 Graeme Orr, *Transcript of Evidence*, 8 May 2014, Brisbane, p. 18.

that there were many problems with the elections there. After postal voting on demand was introduced in the UK in the 1990s we found similar problems with postal vote fraud that created a perception of poor-quality elections in the UK. Only about two-thirds of British people think the elections are fair and that is a dramatic decline compared to previous rates.⁴⁶

- 4.78 Some of the international examples of electronic voting systems cited in Chapter 3, together with security, integrity and transparency concerns more generally, are highly relevant in this context and point towards the serious diminution in public confidence that could result from a failure or irregularity in an electronic voting system, particularly if the system was new. In this scenario public confidence, both in the voting system and the electoral authority, could be destabilised well into the future, and would be very difficult to regain.⁴⁷ The issue of the potential impact of electronic voting is also relative to the amount of trust in the electoral system, and the resultant scepticism that the voting public may have.
- 4.79 Even technology commentators recognise the detrimental impact that electronic voting may have on public confidence in the electoral system:

Democratic legitimacy doesn't just require that votes be counted fairly and accurately, it also requires that they be widely accepted as being fair and accurate. To achieve that level of legitimacy, it's important that every voter be able to understand how the voting process works, so they can have confidence that it will work correctly.

The transparency of paper ballots is a huge advantage here. Everyone understands how paper works, and paper ballots can always be counted by hand if people suspect that counting machines have malfunctioned.

...

Of course, paper elections can be stolen too. But the techniques for stealing elections are more visible and labor-intensive. Generally, to steal a paper election you need to recruit co-conspirators to visit various polling places and modify or replace hundreds of thousands of ballots. For a large election, that requires a sizable operation that's likely to be detected.

46 Sarah Birch, *Transcript of evidence*, 29 July 2014, Canberra, p. 19.

47 International IDEA, December 2011, *Introducing Electronic Voting: Essential Considerations*, p. 6, accessed 20 May 2014, <idea.int/publications/introducing-electronic-voting/upload/pp_e-voting.pdf>.

In contrast, an electronic election allows someone to steal votes silently and invisibly by tampering with a voting machine before the election begins. A single hacker or corrupt insider might have an opportunity to tamper with dozens of machines – especially because some voting machines have been shown to be vulnerable to voting machine viruses that spread from one voting machine to another without any direct human action.⁴⁸

Committee comment

- 4.80 It is important that in embracing technology, the secret ballot is not undermined, voter behaviour is not negatively impacted, and confidence in the electoral process and electoral outcomes is not damaged. At a time of debate about community disengagement with political processes, it would be greatly concerning if the method of voting – the one act of participatory democracy that all Australian citizens will definitely engage in – was to further disengage the community from these processes.
- 4.81 The safety of the system – security, integrity and transparency of the voting process – is critical and must be assured in any electronic system. It is also important that the method of voting is cost-effective. The entire electoral process is undermined if the costs are prohibitively high and becomes subject to ridicule, as occurred in Ireland.
- 4.82 The Committee is of the view that a secure and robust electronic support system is an immediate future goal for democratic practice in Australia.
- 4.83 There is also merit in continued work towards providing a means for a completely secret electronic vote for blind and low vision voters. This should provide a useful platform from which to explore the further development of electronic voting for federal elections.

48 T Lee, 'Hackers probably didn't steal votes today but we'll never know for sure', *Vox*, 4 November 2014, accessed 12 November 2014, <vox.com/2014/11/4/7157807/the-problem-with-e-voting-machines>.

- 4.84 The Committee considers that, to further facilitate access to voting, the current assisted telephone voting system in place for blind and low vision voters should be extended to others with disabilities who would benefit from access to this system.

Recommendation 7

The Committee recommends that the *Commonwealth Electoral Act 1918* and the *Referendum (Machinery Provisions) Act 1984* be amended to allow for expansion of the current assisted telephone voting system to include people with assessed mobility or access issues for the next federal election.

- 4.85 The Committee makes a number of recommendations in Chapter 2 regarding developing electronic support systems for managing the electoral roll and vote count. The Committee is of the opinion that it is more important to direct resources towards developing these electronic support systems than wider electronic, specifically internet, voting options.
- 4.86 The cost of static electronic voting has been proven to be onerous – both in terms of initial investment and ongoing maintenance. While internet voting does not have the same costly associated architecture, its implementation would not negate the need to also provide a widely accessible paper voting alternative for those who do not wish to vote electronically.
- 4.87 Unless universal internet voting was to be made compulsory, which is impractical, this would mean an effective duplication of the voting system in order to ensure that no voter was disenfranchised by the voting method.
- 4.88 Those international jurisdictions that have embraced electronic voting are assessing a balance of risks that does not exist in Australia. They are balancing the need to improve participation against the risk of loss or corruption of votes. A lack of participation is an irrelevant risk in Australia where compulsory enrolment and attendance places an obligation on electoral authorities to provide access to the vote in even the most remote areas of the country. Notably, comparable democracies – New Zealand, the United Kingdom and Canada – have not embraced electronic voting.

- 4.89 The foundations of Australia's voting system – compulsory voting, widespread and easy access to polling booths and polling day held on a Saturday – are robust. Electronic voting would fundamentally change not just the method, but the nature of voting in Australia.
- 4.90 The Committee believes that it is likely that technology will evolve to the point that it will be possible to vote electronically in federal elections. At that stage the question for a future Parliament, and the voting public, will be whether the convenience of electronic voting outweighs the risks to the sanctity of the ballot.
- 4.91 The view of this Committee is that the answer to this question at this time is that no, it does not.

Hon Tony Smith MP
Chair
18 November 2014