2

Electronic voting

What is electronic voting?

2.1   Electronic voting is a general term used to describe a variety of practices
       and technologies that can facilitate voting, recording and counting. Each
       of these is described below:

- Voting — Any system where the elector casts their vote using an online
  system, such as the internet, touch-tone phone voting using interactive
  voice recognition, mobile telephone SMS text facility, or interactive
  digital television. Once recorded, the elector's vote is despatched in real
  time to a secure electronic vote store, where it is held prior to counting;

- Recording — Any system where the elector casts their vote on a voting
  machine (punch card, push button, touch screen). Once recorded, the
  elector's vote is stored in the machine. After voting has concluded, data
  is transferred from each machine to a counting system; and

- Counting — Any system where votes are loaded into a computerised
  counting system, which then tallies the votes and performs subsequent
  actions required by the particular method of voting being used, such as
  eliminating unsuccessful candidates and distributing their preferences
  or striking quotas and transferring the surpluses of successful
  candidates, thereby determining the successful candidate(s). The
  loading of votes can be undertaken in a variety of forms, such as keying
  ballot papers, scanning ballot papers using optical mark recognition or
  optical character recognition readers, downloading data from voting
  machines, or downloading data from an electronic vote store.[1]

---

1   Barry C, Dacey, P, Pickering, T and D Byrne, *Electronic VotingStatus Report 2* (2002), p 3.

2.2   While all of these systems can be collectively referred to as electronic voting, it is important to differentiate between them in discussions of electronic voting experiences in Australia.

Background to 2007 electronic voting trials

2.3   In its 2004 election report, the Joint Standing Committee on Electoral Matters included recommendations for a trial of assisted electronic voting for blind and vision impaired electors and a trial of remote electronic voting for Australian Defence Force (ADF) personnel serving overseas, Australian Federal Police serving overseas and for Australians living in the Antarctic.[2]

2.4   The government response to the committee's report in August 2006 supported the recommendations to establish a trial of assisted electronic voting for blind and vision impaired electors.[3] The government noted that:

> Consultation between the AEC and appropriate organisations is well advanced to allow the AEC to develop appropriate trial arrangements for electronically assisted voting for blind and visually impaired voters to cast a secret printed paper ballot at the next federal election. It is proposed that the trial would be available to eligible electors at 30 pre-poll locations across Australia. The consultations will also inform the AEC's decision on the proposed location of the trial sites and the degree to which the trial could be extended to electors with a print disability.[4]

2.5   While the government also indicated its support for a remote electronic voting trial for selected personnel serving overseas, the scope of the trial was narrowed to exclude Australian Federal Police and people working in the Antarctic:

> The AEC will arrange a trial of remote electronic voting for overseas Australian Defence Force (ADF) personnel, subject to

---

2   Joint Standing Committee on Electoral Matters, *The 2004 election: Report of the inquiry into the conduct of the 2004 federal election and matters related thereto* (2005), pp 135, 258 and 272.

3   Australian Government, 'Government Response to the Report of the Joint Standing Committee on Electoral Matters, The 2004 Federal Election; Report of the Inquiry into the Conduct of the 2004 Federal Election and Matters Related Thereto', pp 15, 19 and 20, viewed on 3 November 2008 at www.aph.gov.au/house/committee/em/elect04/Report/govres.pdf.

4   Australian Government, 'Government Response to the Report of the Joint Standing Committee on Electoral Matters, The 2004 Federal Election; Report of the Inquiry into the Conduct of the 2004 Federal Election and Matters Related Thereto', p 15, viewed on 3 November 2008 at www.aph.gov.au/house/committee/em/elect04/Report/govres.pdf.

satisfactory resolution by the AEC and the Department of Defence of systems and associated security issues. The results of this trial will enable the AEC to inform the development of the broader proposal on remote electronic voting as recommended by the JSCEM. The AEC will keep the Special Minister of State informed on progress and outcomes of the trial and the development of the proposal for the JSCEM.

The Government may consider the extension of remote electronic voting to overseas Australian Federal Police personnel and Australians living in the Antarctic, subject to the outcomes of the ADF trial.[5]

2.6   In addition to the logistical and technical arrangements to support the trials, enabling legislation was required to be drafted and enacted by the parliament. As a precaution against technological solutions not being available within the required timeframe, provisions were included in the Act for the Minister to decide that the voting trials not proceed.[6]

2.7   The bill that became the *Electoral and Referendum Legislation Amendment Act 2007* was introduced in the House of Representatives on 30 November 2006 and was passed by the House on 6 December 2006.

2.8   Upon introduction in the Senate the following day, the bill was referred to the Senate Finance Public Administration Committee. The committee's report, tabled on 20 February 2007, recommended that the Senate pass the bill unamended.[7]

2.9   The bill was passed by the Senate on 26 February 2007 and given royal assent on 15 March 2007.

2.10   Supporting regulations were then developed by the AEC.[8] The AEC noted that due to the complexity and scope of the proposed regulations, the regulations took some time to finalise and that as a consequence of this, the regulations were drafted to commence retrospectively on 1 August 2007.[9]

---

5   Australian Government, 'Government Response to the Report of the Joint Standing Committee on Electoral Matters, The 2004 Federal Election; Report of the Inquiry into the Conduct of the 2004 Federal Election and Matters Related Thereto', p 20, viewed on 3 November 2008 at www.aph.gov.au/house/committee/em/elect04/Report/govres.pdf

6   *Commonwealth Electoral Act 1918*, ss 202AF and 202AM.

7   Senate Finance Public Administration Committee, *Electoral and Referendum Legislation Amendment Bill 2006* (2007), p 6.

8   Australian Electoral Commission, submission 169, p 58.

9   Australian Electoral Commission, *Report into Electronically Assisted Voting at the 2007 Federal Election for Electors who are Blind or have Low Vision* (2008), p 21.

Electronic voting in Australia and overseas

2.11   Electronic voting, particularly electronically assisted voting for electors who are blind or have low vision, has been provided on a restricted basis for a number of state and territory elections. Only in the ACT is electronically assisted voting offered as a voting alternative to the entire community.

Electronically assisted voting

2.12   Electronically assisted voting, which allows people to complete a ballot paper in private, has been a feature of elections in three states and territories in recent years.

2.13   All voters in the ACT have had the opportunity to vote in a limited number of pre-poll voting facilities in the period leading up to polling day and on polling day at elections in 2001, 2004 and 2008.[10]

2.14   In Victoria, electronically assisted voting for electors who are blind or have low vision was trialled for the first time at the 2006 State election. Limited to six locations operating as pre-poll centres in the lead up to the election and on polling day, 199 votes were cast.[11] A Victorian parliamentary committee review of the state election has supported the continuation of electronic voting trials at future state elections.[12]

2.15   In Tasmania, electronically assisted voting for electors who are blind or have low vision was trialled at the 2007 election for the Legislative Council. Only two electors cast a vote using the system at the one pre-poll centre where the facility was available.[13]

2.16   Electronically assisted voting using a range of technologies and devices is a feature of national, state or local government elections in a number of overseas countries including the United States, France, India, and Canada.[14]

---

10   ACT Electoral Commission, 'Electronic voting and counting', viewed on 8 January 2009 at http://www.elections.act.gov.au/elections/electronicvoting.html.

11   Victorian Electoral Commission, *Report to Parliament on the 2006 Victorian State Election* (2007), pp 72–73.

12   Victorian Parliament Electoral Matters Committee, *Inquiry into the conduct of the 2006 Victorian state election and matters related thereto* (2008), p 192.

13   Tasmanian Electoral Commission, *2nd Annual Report 2006-07* (2007), p. 26.

14   ACE Electoral Knowledge Network, 'Countries with e-voting projects', viewed on 10 December 2008 at http://aceproject.org/ace-en/focus/e-voting/countries/.

Remote electronic voting

2.17   Remote electronic voting, whether by telephone, internet or email, is replacing attendance or postal voting for a range of elections in the community including industrial elections and elections for boards of management.

2.18   Apart from the remote electronic voting trial for selected Australian Defence Force personnel serving overseas (examined in chapter 4), there is no remote electronic voting in Australia for state or local government elections. The ACT Electoral Commission has noted that:

> Security concerns and the difficulty of providing electors with unique on-line identifiers are still seen as obstacles that have not yet been overcome. Therefore the Commission continues to hold the view that electronic voting should only be provided in a controlled environment at polling centres.[15]

2.19   Remote electronic voting is a feature of national, state or local government elections in a number of countries including the United Kingdom, Switzerland, France and Estonia.[16]

Where to for electronic voting?

2.20   The committee is mindful of the need to balance the demands for convenient and accessible forms of voting with maintaining trust in the integrity of elections. Experiences and perceptions of electronic voting, both overseas and in response to the 2007 election electronic voting trials, provide important context to assessing the desirability of electronic voting at future federal elections.

2.21   With a range of electronic options now available to vote in competitions and polls (internet, SMS and telephone) and for the election of office bearers in community organisations and corporations (email and internet) it is likely that there will be strong and growing demand for electronic voting in the future.

2.22   While making it clear that they did not endorse any particular voting method and acknowledging that there may be a number of flaws, NSW

---

15   ACT Electoral Commission, 'Frequently asked questions – Electronic voting and counting', viewed on 4 December 2008 at http://www.elections.act.gov.au/faqsvoting.html.

16   ACE Electoral Knowledge Network, 'Countries with e-voting projects', viewed on 10 December 2008 at http://aceproject.org/ace-en/focus/e-voting/countries/.

Young Labor told the committee that electronic voting could increase participation by young people in elections:

> We are simply saying that technology has come a long way and, since there is a lack of participation or a reduction in participation by young people in the system, we think we should be looking at things like maybe online voting or SMS voting—taking that technology that is now available to us and looking at ways that we can incorporate that to improve people's participation in the Australian political system.[17]

2.23   Everyone Counts, a provider of electronic voting services, told the committee about the benefits of remote electronic voting to electors, particularly those in remote areas:

> Internet voting is in broad active use and so far has had quite a high success rate, reaching remote voters in perhaps tens of thousands of elections… ranging from popular voting such as for sporting awards right up to binding elections at the national government level in several countries.

> … Controversy and reported problems around real internet elections are infrequent. In contrast, calls for remote internet voting in the US press in the lead-up to the 4 November presidential elections are gaining in frequency and sonority. The most appropriate group of remote voters to be given a new electronic channel on which to vote is those voters that postal voting most struggles to reach.[18]

Recent overseas experiences

2.24   In the United States, where the use of electronically assisted voting machines (and voting machines generally) is widespread, there is much discussion and debate about the merits of electronic voting. While most of this discussion focuses on the closeness of the 2000 presidential election and concerns with voting machines at this election, debate has continued in recent years despite the replacement of many of the manual voting machines with electronic voting methods. The Institute of Governmental Studies Library of the University of California summarised the different views in the following way:

---

17   Parkin C, NSW Young Labor, transcript, 24 July 2008, p 59.

18   Burton C, Everyone Counts, transcript, 12 August 2008, p 43.

> In sum, views about electronic voting fall into two basic camps. On one side are those who put a premium on accessibility and improving political participation. They welcome electronic voting on the grounds that its advantages outweigh security and reliability concerns — which in their view will always plague voting systems to some extent.

> On the other side are those who put a premium on security and reliability and the need to maintain voter confidence in the electoral process. In their view, unless electronic voting is backed up with a verfiable record of some kind, the risks are too great — the potential for mishap and mischief looms large.[19]

2.25 It is not difficult to find analyses of electronic voting based on US experiences that appear to strongly support either of these two views.[20] It is easy to be persuaded about the relative merits of each side of these accounts. For example, a supporter of electronic voting in the United States noted that:

> Voting fraud can take place with any kind of voting system, including paper ballots. In fact, mechanical voting machines were developed to prevent people from stuffing the ballot box. Electronic machines are even more secure than earlier systems due to sophisticated encryption software and increased physical security of the machines. Although it is true that any computer can be hacked by a dedicated attacker, it is not likely that a hacker would be successful in undermining an entire election. It is more likely that election problems will be the result of untrained poll workers.[21]

2.26 Similarly, it is easy to locate more sceptical views about the security of electronic voting. For example, one author with a background in computer engineering has noted that:

> The use of direct-recording electronic (DRE) voting machines makes U.S. elections highly vulnerable to attack at many points during the voting process. Computer experts have already

---

19 Staff of the Institute of Governmental Studies Library of the University of California, 'Electronic voting: An overview', *Should the United States move to electronic voting?* (2008), p 13.

20 See for example, Henningfield D (ed), *Should the United States move to electronic voting?* (2008); Alvarez R and Hall E, *Electronic elections: The perils and promises of digital democracy* (2008); National Research Council of the National Academies, *Asking the right questions about electronic voting* (2006).

21 Rash W, 'Electronic voting machines are not likely to be hacked', in Henningfield D (ed), *Should the United States move to electronic voting?* (2008), p 25.

> demonstrated the ways that vote-stealing software could be built
> into the machines by dishonest programmers or introduced into
> unattended machines. They have also shown how DREs can be
> infected with viruses and how the central vote-tallying machines
> can be attacked. Any group capable of hacking an election and
> putting themselves into power could maintain that power forever;
> this is the greatest danger of electronic voting.[22]

2.27   It is possible that solutions to technical security issues will emerge as
        newer and better technologies become available. A number of
        non-technical solutions have also been identified as a way of overcoming
        some of the issues, including the use of auditable paper trails, better
        training for polling officials and banning wireless components from voting
        machines.[23]

2.28   The Computing Research and Education Association of Australasia noted
        that internet voting had been criticised in a number of countries where it
        had been used:

> Although internet voting is still being used in some small and
> emerging democracies, and in Switzerland and Estonia, most
> advanced democracies that have trialled internet voting have
> abandoned it. The United States' SERVE project, which was
> specifically for military personnel, was cancelled before
> deployment on the recommendation of the security experts
> commissioned to evaluate it. …

> The government of the United Kingdom recently declared that
> there were no plans to run further trials of internet voting, stating
> "Serious concerns persist about the security and transparency of
> e-voting systems and their vulnerability to organised fraud." A
> French trial of internet voting for overseas French citizens was
> widely criticised and its future is uncertain.

> The concerns about security and transparency of electronic voting
> expressed by experts overseas apply in Australia too.[24]

2.29   It is not clear that continued growth of electronic voting is necessarily
        assured, with the Netherlands, an early adopter of both assisted electronic
        voting and remote electronic voting, recently announcing that electronic

---

22   Stokes J, 'Electronic voting machines can be easily hacked', in Henningfield D (ed), *Should the United States move to electronic voting?* (2008), p 30.

23   Norden L, *The machinery of democracy: Protecting elections in an electronic world* (2007), pp 133–139.

24   Computing Research and Education Association of Australasia, submission 116.2, p 3.

voting was to be discontinued as a result of the identification of security problems with voting machines.[25]

Recent Australian experiences

2.30 Similar concerns, and reassurances, about the security and transparency of the 2007 federal election electronic voting trials and the future of electronic voting in Australia were presented to the committee by providers of electronic voting services and others with technical expertise in computer programming and electronic voting. Where relevant, these are discussed in relation to each of the trials in the following chapters.

2.31 A cautious approach to the adoption of electronic voting was supported by Mr Wen:

> Electronic elections certainly have considerable advantages, and there has been a positive response from participants in the electronic voting trials. But there must be more discussion about the trade-offs between the benefits and the risks. If Australia moves to adopt this new technology, we must exercise great care and caution to limit the risk of electoral fraud and avoid compromising the integrity of our elections.[26]

2.32 A more optimistic view of future arrangements was held by Software Improvements, an Australian-based provider of electronic voting services, which provided an insight into potential developments in electronic voting, with the development of an electronic identification system to enable remote electronic voting.[27]

2.33 Another electronic voting services provider, Registries, told the committee about the momentum that was developing for internet voting:

> Other internet-based elections and pilot results contribute to the notion of a tipping point in the uptake of this technology. In February of 2008, EIC provided the online channel for Democrats Abroad. It was the first time in history that US voters living all over the world were able to remote-vote electronically in a Presidential Primary. Adding the online channel alone increased turnout seven-fold. Voters living in 164 countries, including US Antarctic Territory, were able to cast their votes and be counted.

---

25 Loeber L, 'E-voting in the Netherlands: From general acceptance to general doubt in two years', presentation to the 3rd International Conference on electronic voting, viewed on 10 December 2008 at www.e-voting.cc/static/evoting/files/Session01_LeontineLoeber.pdf.

26 Wen R, submission 181, p 5.

27 Software Improvements, submission 138, pp 5–23.

> While these voters were given the option of voting by post, by fax, by internet or in person, more than 50% chose to vote online.[28]

2.34   A more tempered view of electronic voting was offered by Computing Research and Education Australasia, which highlighted the trust that the voting public must place in voting systems:

> Australians are rightly accustomed to trusting the AEC to handle paper ballots securely, but this trust follows from the transparency of the process: candidates and voters know that scrutineers representing their interests may be present at all stages of the count. Electronic voting requires much more trust, but in Australia has no scrutineers at all. Not only must the voter trust the programmers, the providers of the computers, and the auditors (none of whom are direct AEC employees) to act in good faith, but they must trust them not to make any serious mistakes. Writing secure software is notoriously difficult, as is checking it.[29]

2.35   While not wanting to downplay these concerns, the relatively small scale of the 2007 federal election electronic voting trials, the use of paper output for the electronically assisted voting trial and the use of a more secure electronic network for the remote electronic voting trial rather than the internet, means that some of the general security concerns applying to electronic voting are less of a factor in the committee's deliberations of the trials. However, the committee is mindful that in assessing proposals to expand electronic voting in Australia, greater attention will need to be paid to addressing security and transparency concerns to build trust in electronic voting systems.

---

28   Registries and Everyone Counts, submission 160, p 3.
29   Computing Research and Education Association of Australasia, submission 116, p 2.

A