3

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 voting[47] 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 Bryne, '€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 Bryne, '€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, <electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/Keyfindingsandrecommendationssummarypaper_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/ووینڈ/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.