

Sc



**Australian Government**  
**Department of Communications**

**Drew Clarke**

Secretary

The Hon Mr Tony Smith MP  
Chair, Joint Standing Committee on Electoral Matters  
PO Box 6021  
PARLIAMENT HOUSE ACT 2600

Dear Mr Smith

**Re: Joint Standing Committee on Electoral Matters - Inquiry into the 2013 Federal Election and matters related thereto**

The Department of Communications' submission to the inquiry is enclosed for your consideration. Jointly with the Department of Finance we are responsible for co-ordinating the Government's election policy on e-government and the digital economy. Accordingly this submission focusses on the issue of electronic voting.

Yours sincerely

Drew Clarke  
11 March 2014

FOR OFFICIAL USE ONLY



Australian Government

Department of Communications

# Submission to the Joint Standing Committee on Electoral Matters

March 2014

## Introduction

**This submission addresses the issues and opportunities associated with electronic voting and recommends the Joint Standing Committee on Electoral Matters investigate a potential limited electronic voting trial for the next federal election.**

The rapid acceleration of digital technologies is creating more efficient and convenient ways of completing tasks and accessing services – from paying bills and doing the shopping to lodging Medicare claims and tax returns. However, at the Federal level, Australia still turns to pen and paper for one of our most important tasks: electing our political leaders.

The Electoral Council of Australia and New Zealand (ECANZ) has noted that "it seem would inevitable that paper balloting will, sooner or later, have to be replaced by some form of electronic voting, which may or may not involve the internet". The ACT now uses localised electronic voting for territory elections, and NSW offers electronic voting as an option for voters who are illiterate, incapacitated, disabled and or live in remote areas. This option is also available to blind or limited vision (BLV) voters or are outside NSW on election day. Overseas, Norway and Estonia are leading the way with electronic voting consistent with their leadership position in terms of digital economy matters more generally.

## Electronic Voting

While electronic voting can take a range of different forms, there are two primary types:

- > Local Electronic Voting (LEV): elector presents themselves at an officially designated place to vote using an in-situ electronic device (e.g. kiosks)
- > Remote Electronic Voting (REV): elector casts a vote off-site at a time and place of their choosing, using common devices (e.g. home PC, smartphone).

In September 2013, ECANZ issued a discussion paper on *Internet Voting in Australian Election Systems*. In addition to the quote above some key points made by ECANZ in this paper are:

- > "any risk assessment for the introduction of internet voting needs to be done comparatively: the key question is not whether there are risks associated with internet voting - there clearly always will be - but how the risks and benefits of internet voting compare with the risks and benefits of alternatives."
- > "the most compelling case for the use of internet voting in the short term (assuming the technical concerns can be adequately addressed) would appear to arise in relation to voters for whom it would be a 'game changer': those who cannot otherwise vote at all, or cannot otherwise vote secretly."<sup>1</sup>

---

<sup>1</sup> The Electoral Council of Australia and New Zealand, *Internet voting in Australian election systems*, September 2013, pp. 71-73

## Australian Experience

There are a number of electronic voting trials in Australia and overseas which have succeeded and been integrated with the standard voting system for that location.

### ACT 2001 onwards

Following a close result in the Molonglo electorate in 1998 that revealed a manual counting error, Elections ACT introduced electronic voting and counting for the 2001 Assembly elections. The LEV system has now been used in four elections with only minor changes.

Under the system, select pre-poll and polling day sites use voting machines as voting terminals. Voters have their name marked off the roll and are given a barcode to open a voting session. Votes are stored on a secure local server at the polling place until the close of the election, at which time the data is imported into an electronic counting system. The software used for both voting and counting is built using Linux open source software. The source code is made publicly available prior to the election to ensure transparency in the electoral process.<sup>2</sup>

Positive outcomes from the use of LEV in the ACT include:

- > more timely and accurate counting (no manual counting)
- > fewer informal votes, with unintentional errors almost eliminated
- > greater accessibility for BLV voters and voters who speak a language other than English
- > high level of user satisfaction (in 2004, 86 per cent of voters found it easy to use)
- > increased use of the LEV option (one in four votes in the 2012 elections were electronic votes).

### New South Wales 2011

The *iVote* system was introduced for the 2011 election to allow BLV, illiterate, incapacitated, disabled and remote voters, as well as those outside NSW on election day, to vote using the telephone or internet. The online system was available prior to and on election day. Voters applied to use *iVote* by phone or internet and were supplied with a 6 digit PIN. An 8-digit *iVote* number was later sent via email, mail, SMS or phone. Votes were stored in central servers in two data centres, and were printed at the close of polls to be counted manually.<sup>3</sup> The NSWEC is continuing the development of *iVote* for use in the 2015 NSW general election.<sup>4</sup> Positive outcomes from the use the *iVote* system include:

- > four times the anticipated take up (10,000 votes expected, 46,864 votes recorded)
- > higher voter participation (estimated 30,000 residents may not have otherwise voted)
- > evaluation concluded it was “convenient, reliable and secure”.

<sup>2</sup> Elections ACT, *The 2001 ACT Legislative Assembly Election Electronic Voting & Counting System Review*, 2002

<sup>3</sup> Allen Consulting Group, *Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011*, July 2011.

<sup>4</sup> NSW Electoral Commission, *iVote Strategy for the NSW State General Election 2015: Key Issues, Guidelines, Application Architecture and Voting Protocol*, January 2014

## Australian Electoral Commission (AEC) national trial 2007

Following a recommendation by the Joint Standing Committee on Electoral Matters after the 2004 election, the AEC trialled electronically assisted voting for BLV voters and Australian Defence Force (ADF) personnel during the 2007 election.

The BLV trial was limited to 30 pre-poll sites. Kiosks were used, based on a desktop computer format with a monitor, telephone-style keyboard and headphones. Depending on their level of vision, voters could read the screen or listen to instructional scripts. The kiosk facilitated the vote, but did not store any data. Votes were lodged via a printed barcode, which was then placed in a pre-poll envelope and deposited in the pre-poll box.

The ADF trial was conducted on the Defence Restricted Network. It was limited to ADF personnel with access to the network who were serving in Afghanistan, Iraq, Timor-Leste or the Solomon Islands at the time of the election. Upon completion of the online ballot, voters were given a receipt number which could be entered on a website to confirm their vote was included in the count.

The two trials yielded high levels of user satisfaction and a high number of below the line voters for the Senate, as well as a significant increase in ADF personnel voting. However, infrequent BLV computer users found the kiosks harder to use, while the registration process for the ADF trial (which included mail) was resource intensive. The limited scale of the trials resulted in high costs per voter (\$2,597 for BLV and \$1,159 for ADF). The AEC chose to discontinue the trial.<sup>5</sup>

## International Experience

### Estonia

Estonia is recognised as a leader in REV. It first offered REV for local elections in 2005, before becoming the first country to use it for a general election in 2007. The most recent election in 2011 also allowed for voter authentication via mobile SIM cards. The REV system, called *I-voting*, has its source code publically available.

Internet voting is available for a seven day period prior to the election. Voters use their Estonian ID cards to verify their identity and access the *I-voting* system. Unlimited ballots can be cast, with only the most recent vote counted. A paper vote can also be cast on election day, which will cancel previously lodged online votes. When polling closes, the encrypted votes and the voters' digital signatures are separated to allow for the counting of electronic votes anonymously. Parts of the *I-voting* system are also destroyed in the presence of Electoral Commission members, the auditor and observers to preserve the secrecy of the vote.

The use of *I-voting* amongst participating voters has increased from 1.9 per cent in 2005 to 24.3 per cent in 2011. An assessment by the Organization for Security and Co-operation in Europe found "widespread trust in the conduct of the internet voting", although there was room for further improvement of legal frameworks, oversight, accountability and some technical aspects of the system.<sup>6</sup>

<sup>5</sup> *Internet voting in Australian election systems*, op.cit., pp. 22-23

<sup>6</sup> Organization for Security and Co-operation in Europe, *Estonia: Parliamentary Elections*, 6 March 2011, pp. 1-2

Following a 2011 pilot of internet voting, Norway trialled REV in 12 of its 19 counties for the 2013 parliamentary elections. Norwegian voters could cast their votes in the four weeks before the election and could make amendments by voting a second time (replacing all earlier vote). Voters were identified using one of four authentication options. Over 90 per cent of voters used MinID, the Norwegian Government's digital identity credential, which is also used for a wide range of other government services.

After voting, each voter could download a hash of their encrypted vote, which they could enter at the publicly available digital ballot box to check their hash, and therefore their vote, was registered.<sup>7</sup> The positive reception of the trial led to this being piloted in the 2013 elections as well.<sup>8</sup>

## Drivers

There is an increasing number of factors that suggest a trial of electronic voting should be implemented for the next federal election. These include:

- > **Demand:** Recent federal elections have shown an increase in the take-up of alternative voting options, with record numbers of both pre-poll votes and postal voting. For example, there was an increase of over 300,000 postal votes from 2010 to 2013.<sup>9</sup> The development of REV systems in particular would offer greater access and choice to electors who are normally reliant on pre-poll and postal voting.
- > **Security and reduction of errors:** Electronic voting provides a faster, more efficient and more accurate way of tallying votes than manual counting systems, particularly in closely contested seats.<sup>10</sup> Furthermore electronic voting could include controls to reduce or prevent instances of multiple voting by the same voter and reduce the incidents of unintentional informal voting. In the 2013 Federal Election 5.91% of votes cast for the House of Representatives were informal. This is the highest level since 1984.<sup>11</sup>
- > **Ubiquitous broadband:** Australia now has the highest rate of subscription to wireless broadband services. The development of telecommunications infrastructure means more Australians can effectively engage with government services digitally. This is especially relevant in regional and remote areas where voters must apply for a postal vote or invest substantial time and effort to attend a polling place.

<sup>7</sup> International Foundation for Electoral Systems, *International Experience with E-Voting: Norwegian E-Vote Project*, June 2012

<sup>8</sup> Ministry of Local Government and Modernisation of Norway, *Internet voting pilots announced for 2013*, 14 December 2012, [<http://www.regjeringen.no/en/archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/Nyheter-og-pressemeldinger/pressemeldinger/2012/new-pilot-with-internet-voting-in-2013.html?id=710138>]

<sup>9</sup> Australian Electoral Commission website, *Federal elections*, [http://www.aec.gov.au/Elections/Federal\\_Elections/](http://www.aec.gov.au/Elections/Federal_Elections/)

<sup>10</sup> *Internet voting in Australian election systems*, op.cit., pp. 60

<sup>11</sup> AEC, Virtual Tally Room: Federal Election 2013, <http://results.aec.gov.au/17496/Website/Default.htm>  
Analysis of Informal Voting, House of Representatives, 2010 Federal Election - Informal voting at House of Representatives elections, Updated [30 May 2013], [http://www.aec.gov.au/about\\_aec/research/paper12/hor.htm](http://www.aec.gov.au/about_aec/research/paper12/hor.htm)

- > **Development of supporting 'soft' infrastructure:** The rapid take-up of the myGov online portal indicates that there is considerable demand for online government services. The Government has committed to offering individuals and entities a secure digital inbox.<sup>12</sup> The myGov portal, with its associated credential and digital inbox, or other secure in-boxes that are emerging, could provide a secure digital channel for the AEC to communicate with the electorate and form part of the service delivery model for an electronic voting trial.

## Risks and Mitigation Strategies

- > **Cost:** While there will be initial set up costs in installing any new system, it is important to note that as the number of people using the system increases, this will lead to a decrease of costs-per-voter. ECANZ also predicts that "Once an internet voting system is put in place, the unit cost of each vote cast is likely to be substantially lower than the unit cost of ordinary or postal votes".<sup>13</sup>
- > **Coercion:** Voters in private environments such as a home or office could be more vulnerable to coercion or intimidation to vote in a manner not of their choosing. It is noted however that this risk is also present when postal voting. The success of postal voting indicates that the risk of coercion is not sufficient to invalidate the voting method. For REV, this concern may be mitigated through an REV system like Estonia's, which allows for re-lodging of votes. This ensures a voter can lodge their vote as many times as they would like and only their last vote will be counted. Voters are also able to replace electronic votes with a vote submitted in-person in an environment which prevents coercion.
- > **Anonymity:** Concerns have been raised around retaining voter anonymity to ensure votes cannot be linked back to the voter. These concerns can be mitigated by ensuring a vote is not linked with the identity verification process, or by decoupling the data after a vote has been cast. For example, the NSW iVote system mitigates this risk by printing the votes anonymously at the end of the election and destroying the data after results are officially declared, for added security. Estonia and Norway have also developed means of addressing this risk.
- > **Identity verification:** All voters – whether voting online, by post or in person – must be identified to ensure that every voter votes and only votes once. A range of identification methods have been used to ensure that identification is accurate. In Australia, the AEC 2007 trial and the NSW iVote system use two-factor authentication based on physical identification to verify a voter's identity. The AEC may consider alternative possibilities that use existing online services such as myGov to confirm voter identity.
- > **Security:** Security concerns raised in relation to electronic voting include remote hacking of data via the internet or hijacking of programs used to administer the voting. These risks can be mitigated through adherence to best practice for remote access to secure systems, such as the use of two-factor authentication and dynamic IP addresses. Some trials have also published the REV system source code to encourage white hat hackers to test for security faults, though the NSW Electoral Commission's *iVote Strategy for the NSW State General Election 2015* argues that the availability of REV source code should be limited to trusted REV experts.<sup>14</sup>

<sup>12</sup> The Coalition's Policy for *E-Government and the Digital Economy*, p19.

<sup>13</sup> *Internet voting in Australian election systems*, op.cit., pp. 18

<sup>14</sup> *iVote Strategy for the NSW State General Election 2015*, op. cit., pp. 7-8

## Conclusion

Electronic voting systems and processes have improved considerably in recent years. Given the strong voter demand for convenient and accessible voting options, there is merit in undertaking a limited electronic voting trial at the next federal election. While there are risks associated with electronic voting, the analysis above suggests that it is at least consistent with, and probably less than existing channels. The department understands that there will be costs associated in implementing a trial and how this is met would be considered by agencies in scoping the trial. A limited trial will assist in building the corporate knowledge and systems necessary to reliably scale electronic voting channels in future elections. However for a trial to be in place for the next Federal election the necessary detailed planning and design work will need to commence in the near term.