F2012/54

13 July 2012

Mr Jai Rowell MP
Chair
Joint Standing Committee on Electoral Matters
Parliament House
Macquarie Street
SYDNEY NSW 2000

Dear Mr Rowell

Review of the *Parliamentary Electorates and Elections Act 1912* and the *Election Funding, Expenditure and Disclosures Act 1981*

I write regarding questions taken on notice at the Joint Standing Committee on Electoral Matters (JSCEM) Hearing held on 15 June 2012.

The answers are provided in order in the Attachment.

Yours sincerely

Colin Barry

Colin Barry
Electoral Commissioner

Attachment

1. What was the informal vote in the Upper house (transcript p 5)?

For the NSW State General Election 2011 the informal vote in the Upper House was 230, 261 (5.35%) this informality rate is a slight improved from 2007 where the upper house informality rate was 6.11%. We attribute this improvement to changes made by the NSWEC in the ballot paper layout and improved information provided NSWEC to the public on how to complete an upper house ballot paper.

2. Can you provide the Committee with a copy of the Procedure Information Technologies Conditions of Engagement document (transcript p 20)?

The information on the iVote contract was provided to the JSCEM by email to Mr Rohan Tyler on 27 June 2012.

3. How easy is it for persons, who have obtained an AVO against another person, to apply for a postal vote (transcript p 64)?

A person who believes that attending a polling place will place them in danger can apply for a postal vote under the *Parliamentary Electorates and Elections Act 1912* No 41, Part 5, Division 9,

114A Application for a postal vote certificate and postal ballot paper;

(1) An elector who:

(j) believes that attending a polling place on polling day will place the personal safety of the person or of members of the person's family at risk, may make an application for a postal vote certificate and a postal ballot paper to the Electoral Commissioner.

4. Does Norway set a desirable standard for NSW in terms of how transparency can be achieved in e-voting (transcript p 67)?

The New South Wales Electoral Commission (NSWEC) believes the Norway project provides useful information to assist NSW determine the most appropriate way of increasing transparency for iVote. However, we do not believe the approach taken in Norway should be adopted as best practice. As outlined below Norway did not achieve all the outcomes they hoped to achieve with the approach they took.

The following is an extract from one of the evaluation reports prepared for Norwegian evote project[1]. This report identifies how contentious the issue of source code access is and identifies many of the factors influencing decisions regarding source code availability.

> *There are two aspects to the transparency of information related to the Internet voting system: access to the information itself, and the ability to disclose the findings of analysis conducted on the basis of this access. Both are important for the overall transparency of the system, and in order to enable trust in the system.*

[1] "International Experience with E-Voting", Norwegian E-Vote Project, Jordi Barrat i Esteve, Ben Goldsmith and John Turner, June 2012, IFES, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf

Access to information can be a touchy issue from a number of aspects. System administrators may be unwilling to disclose all aspects of a system as doing so may make it easier for people to manipulate and defraud the system. A common demand by stakeholders is that the voting system source code is made available for public scrutiny. The purpose of this disclosure is to allow stakeholders to review the code and identify any instances where the system does not function correctly, either because of a mistake or a deliberate attempt to manipulate the system. Suppliers are often reluctant to provide this access as they consider the code to be proprietary in nature and the result of significant investment on their part. Similarly, certifying/reviewing organizations may be unwilling to disclose all aspects of their work as this may provide information on the methodology that they use, which could be useful to competitors. In fact, significant debate has taken place around the merits of disclosing source code. The issue of system security is obviously very important but the general tide of opinion seems be moving towards making electronic voting, and Internet voting, source code accessible. While the publication of source code is an obvious transparency mechanism and one which may represent an important cue conveying trustworthiness, its actual impact may be less significant for a number of reasons. Only a small percentage of IT-literate stakeholders will be able to review the source code in any meaningful manner.

Furthermore, as code for systems such as Internet voting will be complex and long, a full review of the source code will represent a significant investment in time and effort. This may be an investment that few, if any, are willing to make on a voluntary basis. Stakeholders such as political parties and observers may be willing to employ IT experts to conduct a review of the source code, but it is also possible that, even when source code is published, no one will conduct a meaningful review of it. Nevertheless, the mere fact that source code is published may serve as a deterrent against the deliberate manipulation of the Internet voting system. However, the publication of source code will not help to identify genuine mistakes if it does not lead to competent stakeholders reviewing the code.

One of the ways that Internet voting suppliers can try to mitigate the commercial risk of providing access to their source code is through limiting access to those willing to sign a non-disclosure agreement (NDA). NDAs limit the information that those reviewing the code can disclose. While such agreements may help to meet the conflicting demands of transparency and commercial interests, they are not without their problems especially where they overly limit the possibility for reviewers of the code to publish the results of their review.

The following are relevant extracts from the recently published audit report on the Norwegian election by IFES[2], which deals with the availability of source code. This report used the Council of Europe Recommendation for e-voting[3] as a framework for

[2] Compliance with International Standards Norwegian E-Vote Project, Jordi Barrat i Esteve and Ben Goldsmith, June 2012, IFES
http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

[3] Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting
http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/

assessing the Norwegian project. The bolded headings below are the relevant recommendations related to Public Confidence (PC).

It is interesting to note that it was very difficult for the Norwegian project team to make the source code available in a timely manner and in fact the final release of the code occurred after the election. NSWEC believes this issue would be the same for the iVote system which also uses complex technology and multiple systems some of which could be updated during the election configuration process which means that it is unlikely a public assessor could effectively assess the code in time to give meaningful feedback to the NSWEC prior to the system going live.

> ***Public Confidence (PC) / 21. Information on the functioning of an e-voting system shall be made publicly available.***
>
> *Transparency has been a guiding principle in the Ministry's implementation of the Internet voting system. The Ministry's website has many pages with information on the Internet voting project. This includes technical documentation, including the source code for the voting system, as well as presentations on the features of the Internet voting system.*
>
> *While all relevant information seems to have been publicly available, timing constraints led to some limitations in the availability of this information. The first version of the source code was published on the Ministry's website on June 7, 2012 (typo should be 2011), and the Ministry made it clear that there may be updates to this version. Updates were in fact made subsequent to this as bug fixes were made to the system. Crucially, the final version of the source code was not made available on the website until October 7, 2012(typo should be 2011), nearly one month after the election. The Ministry indicated that anyone who wanted to see the final version of the source code before it was posted online would have been provided access, but many would have expected the version on the website at the time of the election to be the final version.*
>
> *The source code is a vital component of the information related to the functioning of the Internet voting system. There is no indication that the failure to publish this information prior to the election was an attempt to mislead stakeholders in any way. In fact, the Ministry made significant efforts to provide as much access to information as possible. The complexity of the Internet voting system and late changes that had to be made to it meant that the Ministry was focused on making the election happen at the expense of immediately publishing the new version of the source code.*
>
> *Nevertheless, the failure to have the source code published represented a failure to provide key information on the system in a timely manner and provide those stakeholders with an opportunity to review this key information before the election took place.*
>
> *The Norwegian Internet voting system is partially compliant with this recommendation.*

The observations below identify how difficult it is to provide all the source code for the system. Indeed one issue that the Norwegians faced was what is the scope of the eVote system and how much code can and should be provided to ensure the voting was transparent but did not disrupt the operation and contractual obligations of other systems. Norway found that parts of the eVote system could not be provided because they related to some of their existing systems which were used to identify electors and as such considered confidential.

PC / 24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.

The Ministry required the full disclosure of the source code in the Regulations Relating to Trial Electronic Voting (art. 28.2) and it also uploaded to the website the documentation generated during the tender, including the technical specifications presented by the suppliers. The regulation also foresees the publication of "the requirements relating to the solution (infrastructure, servers, data in the system, procedures, guidelines for deleting return codes, roles, access, technical documentation, testing, time plans, security copying procedures, etc.)" (art. 27.1) as well as the "documentation relating to how the system has been built up and how it works, including detailed specifications and architectural documents" (art. 28.1).

However, some technical components, like the authentication mechanisms, remain outside the scope of this policy as they are managed by other institutions that did not disclose details of their systems to the Ministry. This recommendation could be considered as having been met if we considered the authentication mechanisms as not being "components of the voting system." However, as the authentication of voters is an inherent and critical component of the Internet voting system, this option does not seem acceptable.

The failure to provide access to the components of these authentication mechanisms does need to be contextualized. The other Ministries and agencies responsible for the authentication mechanisms, MinID, BuyPass and Commfides, are all subject to regulation and are audited on a regular basis. Therefore, while the components of these systems are not made available to the competent electoral authorities, as required by the recommendation, they are subject to oversight.

The Norwegian Internet voting system partially complies with this recommendation.

The section below outlines the extent of the publication and the transparency undertaken by Norway. Note the NSWEC has indicated it is willing to publish much of the documentation surrounding the iVote system but believes the publication of source code will be of little practical value and only create an additional cost and burden to the project. In particular the NSWEC is concerned that the publication of source code will result in a large number of requests for information. It should be noted that the Norwegian project cost was several times that of iVote.

PC / 69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.

The Ministry published more information regarding its Internet voting system than any country which has so far used Internet voting. We know for instance that the system comprises the following key components:

- *Voter's Computer: Downloads and runs the voting client application (Java Applet).*
- *Electoral Roll (ERoll) Service: Holds information on the electorate.*
- *Authentication Service: Holds and sends voter credentials to the voter's computer (upon successful authentication by MinID, BuyPass or Commfides).*
- *Vote Collection Service (VCS).*
- *Return Code Generator (RCG).*
- *Key Management Service (KMS): Creates and distributes keys. It is also in charge of establishing the private key used for decrypting the votes.*
- *Cleansing Service: Discards electronic votes (e-votes) of voters that cast a paper vote (p-vote) and all but the last e-votes in the case of voters having cast more than one online vote.*
- *Mix-Net: Mixes and re-encrypts the encrypted votes signs the output.*
- *Decryption / Counting Service.*

Except for the electronic electoral roll service (developed by Ergo), all of the systems listed above run software developed by Scytl.

The source code for the Internet voting system and its licence has been published (although the code available online at the time of the election was not the final version), as well as all documents regarding the tenders (the tenders themselves, their evaluation and the auditions of the tendering companies as webcasts), the contracts, the system's specifications and the description of critical components (system's interface with the ID portal, interface for transfer of results to the Election night system, etc.).

The installation date of the various software components is available from the documents accessible on the web page.92 An issue tracking tool is also online at https://source.evalg.stat.no/*. Therefore, it can be said that Norway has done much to comply with this recommendation.*

Yet, as Spycher, Volkammer and Koening rightly note[93], "trust among the full population will be supported by publishing a simplified system documentation that explains and if applicable quantifies the remaining measures for trust establishment. Independent experts who have assessed the full documentation would need to confirm that the simplified documentation has been derived correctly." However, Spycher, Volkammer and Koening note that "it would be beneficial to additionally relate the explanations to a security concept and underline how and to which degree the security requirements are met."

The last point of the recommendation stating: "a procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time" does not appear to be covered in the Norwegian case, especially as the explanatory memorandum makes it clear that this should be possible for authorities and citizens alike.

It is clear that while significant efforts have been made to meet this recommendation, there are still some additional steps that could be taken.

The Norwegian Internet voting system partially complies with this recommendation.

The requirement below was satisfied by the NSWEC by publishing the vote preference data which then allowed members of the public to write their own software and verify the count was done correctly. It should be noted that the decision to publish preference data was as a result of similar decisions by the AEC and VEC.

FC / 98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.

There are a number of ways in which the Norwegian Internet voting system can demonstrate that the counting process accurately counts votes. Firstly, it publishes the source code for voting system so that those able to analyse the source code can check that the system has been designed to count the votes accurately. In addition to this, the implementation of E2E verification mechanisms can demonstrate that, in practice, votes were processed accurately through the counting process. As discussed in other recommendations, the audit of these E2E verification mechanisms showed that votes were counted accurately.

The counting can be reproduced and, in fact, the Norwegian government conducted both a preliminary count and a final count of Internet votes (although there were differences due to the differences in the data on paper ballots cast). However, the explanatory memorandum indicates that, "to gain confidence, it is most important that the counting process can be reproduced and that this can be done with a different system from a different source" (italics added).

Taking into account the publication of the source code, the counting could be reproduced by anyone and with other means. It is worth wondering whether any election management body would be willing to provide vote data, even if encrypted, to 'another source' to replicate the counting process. Compliance with the wording of the explanatory memorandum would appear problematic from a data security and confidentiality perspective. However, the recommendation only requires that the counting of votes be reproducible, not that it actually be reproduced.

The Norwegian Internet voting system complies with this recommendation.

Given the above the NSW Electoral Commission agrees with the evidence given by Dr Teague of CORE to the Victorian Electoral Matters Committee hearing[4] for the 2010 Victorian state election in relation to making source code publically available.

Dr TEAGUE — And the source code, yes. This is a very vexed issue, and not just to me. This issue is being batted back and forwards throughout North America and Europe and everywhere else. The thing that makes something secure is having lots of people look at it really carefully, so it would be wrong to say that publishing the source code automatically makes it secure. It does not, unless publishing the source code encourages more

[4] Victorian Electoral Matters Committee hearing for the 2010 Victorian state election http://www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/Corrected_Evidence_2010_Vic_State_Election_23_August.pdf

> *people to actually have a careful look at it and tell the VEC about the bugs that they find and so on.*

Given the above information the NSWEC believes that unfettered access to source code by the general public is not the way to increase transparency.

The NSWEC proposes that expert reviewers have access to the source code under an NDA. The findings from these reviews will then be published on the NSWEC website along with NSWEC comments and a statement of conflict of interest and reviewer resume. The resume will outline the "expert" reviewer's eVote credentials thus allowing an informed assessment of the findings by the public.