13 December 2018 (last revised 16 December 2018)

Online voting expert calls for Royal Commission into the cyber security of Australia's electoral system and critical infrastructure

iVote Report published -- the one expert submission that was not

Ralph McKay, founder and CEO of leading online election service provider, BigPulse.com, says, "The NSW Electoral Commission's conduct in relation to the Wilkins iVote inquiry is typical of a culture that has caused trust in Australia's institutions to hit an historical low".

The Wilkins Report stresses the importance of transparency in the iVote project. Yet the NSWEC waited six months before publishing it -- curiously coinciding with McKay's FOI request deadline for access to the iVote report.

Ten submissions were made to the iVote inquiry. Wilkins asked that all submissions be published. Nine were published with the publication of the report. McKay's submission was not published. Why was one expert submission not published? The iVote inquiry was promoted as "independent". McKay believes an "independent" inquiry should not give the NSWEC discretion to overrule Mr Wilkins' request for publication of all submissions.

McKay has not received an explanation but notes the NSWEC gave a strong hint by asking if he would consider redacting a small but critical part of his submission. The text the NSWEC expressed interest in redacting relates to questions McKay raised about the independence of the inquiry and comments made by Professor Rodney Smith in an email he sent to McKay in 2016. Professor Smith is one of the members of the NSWEC appointed three person iVote inquiry "expert panel". Professor Smith is also a long term advisor to the NSWEC on voter coercion matters.

McKay believes the quoted comment from Professor Smith implies the existence of a deeply concerning privacy flaw in the iVote system -- a flaw with the potential to cause emotional or even physical distress for vulnerable electors. McKay also says that if Professor Smith has unwittingly misrepresented the iVote design then it implies the existence of a different type of design flaw. This would mean the iVote "vote counted verification service" does not reliably inform electors if their intended vote was actually counted and exposes all electors using iVote to undetectable impersonator re-votes!

It seems therefore that the NSWEC iVote team have an extraordinary dilemma -- a choice between one of two basic security flaws related to the use of re-voting. The Wilkins inquiry report, requested by the NSW Parliament, is silent on the issue.

No one on the iVote inquiry NSWEC appointed "expert panel" is an expert in the highly specialized field of online voting security. Not surprisingly, NSWEC accepted 28 of the report's 29 recommendations.

What the NSWEC wanted to redact from McKay's submission

On 22 May 2018 the NSWEC stated in an email to McKay, "*Mr Wilkins has asked the NSWEC to publish all submissions received on the same page of the NSWEC website that his report will also be published*." The statement was repeated in another email sent 28 Nov 2018.

In its November 28 email the NSWEC stated, "*We wish to obtain your view about the two items highlighted on pages 6 and 7 (attached). Specifically, we ask that you give consideration as to whether you would redact the highlighted text.*"

The NSWEC redaction requests related to comments referring to Professor Rodney Smith. The text the NSWEC highlighted in McKay's submission is,

"*It is difficult to understand how Professor Smith can be considered "independent" when he has a long association of providing consulting expertise to the NSWEC."*

And also the following text copied from an email McKay received from Professor Smith in September 2016, in which Professor Smith stated,

"*<u>You are right that the receipt gives a coercer an opportunity to find out that someone has re-voted</u> but the re-vote mechanism gives the voter opportunities to resist coercion by re-voting that someone who is voting by post or at a polling place does not have.*"

McKay responded asking the reason for the redaction requests but received no answer.

Why the hidden text matters

The underlined portion of the text in Professor Smith's email to McKay is critically relevant to the suitability of the NSWEC's iVote technology for use in government elections. If Professor Smith expressed a correct understanding of the iVote re-voting mechanism in his email to McKay then it points to a deeply concerning privacy flaw in the iVote system. It exposes vulnerable electors to retribution from unstable coercers. A flaw which McKay believes has the potential to cause emotional of even physical distress for vulnerable electors -- as discussed in his unpublished submission attached.

A further dilemma for the NSWEC iVote team is that if Professor Smith's email to McKay in fact misrepresented the iVote re-voting mechanism -- that is, if the receipt code does not in fact give coercers an opportunity to find out if someone they coerced has re-voted -- then it strongly suggests that iVote is not strictly issuing each vote with a unique receipt code. This would imply that iVote's "vote counted verification service" is more deeply flawed than many interested experts have assumed. Not issuing unique vote receipt codes would mean iVote's vote counted verification service does <u>not</u> inform electors if their intended vote was counted. It would mean the iVote vote counted verification service is a deception -- it informs that someone's vote was counted, but not necessarily the elector's intended vote! Clearly electors would assume the verification service informs them if their intended vote was counted or not. This design would also mean all electors using iVote are exposed to undetectable impersonator re-votes.

McKay has been attempting to discover since early 2015 which of these two security flaws exist in the NSWEC's iVote technology. This clash between two different security objectives is ignored in the Wilkins report. McKay believes the Wilkins report should have expressly reported on these basic security issues as discussed in his submission. To the experts the evidence is overwhelming -- one of these two security flaws does exist in iVote.

McKay says, one way to resolve this dilemma is to make the absurd assumption, implied in the Wilkins report, that: voter coercion does not exist in Australia, will not exist in the future, and certainly does not exist in the homes of people at risk of domestic violence, and that the secret ballot also known as the "Australian Ballot", has no relevance to Australia.

In fact McKay did discover odd drafting in the NSWEC's literature following the NSW State Election 2015 that appeared consistent with iVote not issuing unique receipt codes -- as discussed in McKay's earlier published submission to the 2015 NSW State Election and Related Matters inquiry.

Interestingly, the published submission to the iVote inquiry from Dr Roland Wen and Prof Richard Buckland states,

"*.. in iVote the votes can be changed without changing Receipt Numbers, and so checking Receipt Numbers does not help detect such changes to votes.This vulnerability is partly caused by a design flaw in the Verification Service from the first version of iVote in 2011*".

Critical statistics withheld

These particular security issues both relate to the use of re-voting and illustrate the importance of the iVote re-vote statistic, which was ignored in the Wilkins report.

The re-vote statistics, that is the number of re-vote requests and actual re-votes, is vital for understanding the success of the verification process, and coercion management. On re-voting the Wilkins report states simply, "*The iVote system itself allows a voter to change their vote and cancel their previous vote*". The NSWEC has never released the re-vote stats.

McKay says, “the use of re-voting contains many traps for the inexperienced”.

Lawmakers and the public misled

McKay believes that by not publishing his submission the NSWEC has misled the NSW Parliament and the local and international communities and media groups following this inquiry. It has given a false impression of the real expert opinions, through the ten submissions made to it, that informed the panel conducting this inquiry. It also hides from the public issues which go beyond vote security to include elector security and conflict of interest concerns.

McKay believes, "A reasonable, diligent and independent person reading both the hidden submission and the Wilkins report would conclude that the issues raised in the hidden submission were dismissed without explanation. Not publishing all submissions denies others the opportunity to see this."

McKay says, "A genuine independent inquiry with the integrity of a Royal Commission would not shield the NSWEC from scrutiny or give a false impression of expert opinion on vote security."

Online voting has been McKay's dedicated profession for the past 18 years. He feels the NSWEC's discriminatory treatment of his expert submission cannot be justified and not in the public interest.

Wilkins report airbrushed the elephant in the room

McKay says, "Like the study of consciousness, online voting security comprises a relatively easy problem and an intractable hard problem. The Wilkins report focused on the relatively easy problem -- that is, typical issues common to cyber security in general. The Wilkins report ignored the elephant in the room, the hard problem. The hard problem is: how to produce a genuine transparent vote counted audit together with protection of vote secrecy and coercion management using re-voting."

The Wilkins report dedicated less than three pages to end to end verification, in a 45 page report plus appendices. McKay says, "The iVote report just tinkers around the edges of the so called iVote verification technology -- a staggeringly unsafe and misleading technology."

Examples of electronic election verification basics ignored by iVote and the Wilkins report:

- a complex black box cannot be trusted to verify itself, the iVote method assumes the black box always tells the truth;
- real verification requires the issuing of full tamper proof vote receipts each with unique receipt codes;
- real verification requires the publication of all counted vote receipts immediately after vote close;
- real verification requires a statistically significant number of electors to confirm that their vote receipt with intended preferences is included in the published list;
- it is easy to corrupt the vote count and transparent verification process by not issuing unique receipt codes.

“Staggeringly bad” say leading independent academic experts

It's apparent the independent academic experts, with the most relevant network security qualifications, who also made submissions to the Wilkins iVote inquiry were not impressed either: Dr Chris Culnane, lecturer at the University of Melbourne, researching verifiable voting, privacy and cyber security tweeted, "*a staggeringly badly written report. It fails to grasp the technical challenges or coercion risks. It dismisses experts in the field with statement wholly lacking in justification*."

Dr Culnane's tweet no doubt expresses the feelings of the many leading network security academics who contributed to the Teague, Culnane et al submission and other leading network security academics across the world with specialized understanding of electronic voting.

Cyber security of Australia’s electorate system – needs real independent inquiry

McKay believes the Wilkins report is likely to do more harm than good because it allows the NSWEC the freedom to continue with the deception that the iVote technology is safe.

The report makes naive assumptions about the motivation of cyber criminals and state actors to interfere with election results. It makes naïve assumptions about the relative risks of postal voting compared to remote online voting in government elections. It is obvious that the voice of real experts, academics and practitioners, in online voting security were ignored. It is clear that no-one in the NSWEC appointed “experts panel” understands the “hard problem” in remote online voting.

McKay is calling for a Royal Commission into the cyber security of Australia's electoral system and related critical infrastructure.

ralph@bigpulse.com