Rejoinder To A Statement By The NSW Electoral Commission

On 21 September 2015, the NSW Electoral Commission (NSWEC) published a statement on their website, entitled Response from the NSW Electoral Commission to iVote Security Allegations\(^1\) (for convenience, the “Response”). This statement “concerns allegations made during the NSW 2015 state election regarding the security and integrity of the Commission’s iVote® internet voting system by researchers Dr Halderman (University of Michigan – USA) and Dr Teague (University of Melbourne)”. The latter, Dr Vanessa Teague, an academic in the Department of Computing and Information Systems, is an expert in the technology and principles of electronic voting.

The University of Melbourne welcomes open discussion of the topic of electronic voting. However, the NSWEC’s statement is published in their privately managed forum, which is not designed for support of discussion or rejoinder, and, despite the official nature of the statement, is opinionated – indeed, the CIO of the NSWEC explicitly stated that the Response was due to their “views”, and is intended to publicly spell out their concerns with Dr Teague’s conduct.\(^2\) This is despite the fact that the University had already provided responses to NSWEC rebutting these concerns. The Response can be viewed as an attack on an independent scientist, and contains significant misrepresentations of the work and activities of Dr Teague, as well as errors of fact.

This rejoinder is a defence of Dr Teague, and corrects these misrepresentations and errors. Dr Teague is an outstanding researcher who has given expert advice to Australian governments on the topic of electronic voting for several years, a recent example being her Submission to the NSW JSCEM Inquiry Into The Conduct of the 2015 State Election.\(^3\) Dr Teague’s research activity is concerned with mechanisms for conducting elections using electronic systems, a topic to which she has made numerous positive contributions, for example suggesting methods by which the integrity of elections can be protected.\(^4\) Such research necessarily rests on a deep understanding of the possible shortcomings of electronic voting systems, and it is this understanding that has informed Dr Teague’s critiques of the specific mechanisms used in the 2015 NSW election;\(^5\) without this intervention, most of iVote’s 280,000 votes would have been vulnerable to attack. She is motivated by a commitment to the long-term integrity of Australian elections, a commitment expressed not only in research papers on verifiable elections, but in her substantial contributions to the design of the Victorian Electoral Commission’s at-the-voting-booth supervised electronic voting system, organised by Mr Craig Burton. There is strong support of the work of Dr Teague, and of her colleagues in this work including Dr Alex Halderman and Professor Rajeev Goré, from the international scientific community.

---


\(^2\) The CIO, Mr Ian Brightwell, wrote to us to alert us to the Response. The entirety of his explanation of the Response is: “We certainly do have very different views on a range of issues. I suggest you have a look at our recently updated response which sets out how we view the issues and spells out our concerns with Vanessa’s conduct.”


---

Department of Computing and Information Systems
The University of Melbourne, Victoria 3010 Australia
T: +61 3 8344 1500   F: +61 3 9349 4596
It is of particular concern that the errors and misrepresentations in the Response are present despite NSWEC having had good opportunity to examine and correct them prior to publication. The matters in the Response had previously been raised with us in a formal complaint by Mr Ian Brightwell, Director IT & CIO of the NSWEC, on 26 March 2015, and in private correspondence on 2 September 2015. These were addressed by the University in, respectively, a formal response on 19 June, and a detailed response to the private correspondence on 11 September. The NSWEC, however, then proceeded to make a public Response on 21 September containing many of the same errors and misrepresentations. Mr Brightwell, in alerting us to the publication of the Response, did not explain or indicate any respect in which the University’s defence of Dr Teague was mistaken, and stated only “we certainly do have very different views on a range of issues”.

We welcome the initiative of the NSWEC in their willingness to trial and deploy electronic voting systems. We believe that electronic voting is an inevitable component of our elections, as well as a potential enabler of new forms of democracy, and it is forward-looking to investigate such approaches.

However, if electronic voting is to be used, it must be robust; for example, a flawed system in which large numbers of votes were untrustworthy would render elections meaningless, especially in contexts where only small numbers of votes can sway the outcome – as has been the case in several recent Australian elections. The integrity of voting systems is fundamental to the operation of a democratic society. We regard frank, disinterested examination of topics such as potential flaws in voting systems as a key role of a publicly engaged institution such as ours. Internet voting has the potential to dramatically disrupt our electoral processes – as it shifts votes away from the booth, off paper, and away from election day, and to connected devices that are used for a wide variety of other purposes – and it essential that we have the same trust in such systems as we do in existing, paper-based methods.

I now address some of the specific points raised in the Response.

In the Response, the NSWEC state that on 20 March 2015 Dr Teague alerted the media and CERT Australia of problems in the iVote system, but did not provide a report to NSWEC. This statement in the Response omits the fact that Dr Teague notified NSWEC of various separate problems in the iVote protocol some 18 months before the election, in August 2013, but did not receive a response other than a formulaic acknowledgement of receipt. Given NSWEC’s previous lack of action, Dr Teague and Dr Haldeman judged that a direct report to NSWEC might not receive sufficient attention, and took a responsible course of action in contacting the Australian CERT, which is the appropriate authority for notification of live security vulnerabilities. The press was also notified; we regard briefing of journalists under strict confidentiality and embargo as a justifiable component of responsible disclosure, as this is a matter of significant public interest. Use of embargo meant that Dr Haldeman and Dr Teague ensured that iVote’s FREAK vulnerability was not made public until after the problem was rectified.

The Response notes that “the vulnerability was found by Drs Teague and Halderman using a free internet based certificate test service, which is a tool commonly used by system administrators to test website security”. We interpret this as agreement that the vulnerability was a serious one, as it means that discovery of the vulnerability was elementary. The fact that “to have had a significant effect on the election a number of other difficult to implement factors would also have needed to be present” is not reassuring; it appears that a determined aggressor could have distorted the election outcome.

It seems that the NSWEC shared this concern, because the vulnerability was immediately closed, though not before 66,000 votes had been cast. Without the work of Dr Teague, the integrity of most of the 280,000 online votes would have been open to question.

It is asserted in the Response that “this significant information was known by Drs Teague and Halderman soon after voting commenced, at 8am on Monday the 16th of March”. This is incorrect. The response further asserts that “it has been subsequently confirmed from statements made by Dr Halderman ... that the existence of the FREAK vulnerability was known to him before Wednesday the 18th of March”. This is misleading. Dr Teague and Dr Halderman discovered during the voting period that the iVote system was vulnerable to serious flaws in its cryptography, including vulnerabilities to attacks known as ‘FREAK’ and ‘Logjam’. The FREAK vulnerability is a general weakness in some online security implementations, and was publicly known from 10 March, but not known until later to apply to iVote. It took several days to confirm that these vulnerabilities could be used to steal votes, and to document the technical problems in a way that would help the election authorities to correct them; they then immediately notified CERT.

The Response asserts that “The Commission has never claimed that the operation of the iVote system was completely risk free”. This is incorrect. Mr Carroll of the NSWEC was quoted by the ABC on 4 February 2015 as saying that “People’s vote is completely secret. It’s fully encrypted and safeguarded, it can’t be tampered with, and for the first time people can actually after they've voted go into the system and check to see how they voted just to make sure everything was as they intended.”

The Response lists six points in defense of the robustness of the iVote system. However, some of these points have already been rebutted to the NSWEC, and it is surprising that they are repeated in the Response when they are, in some cases, known to be factually incorrect. For example,

- The response asserts that the “verification service allowing voters to verify their vote was captured by iVote as cast”. However, the paper by Dr Haldeman and Dr Teague described multiple methods of circumventing this verification mechanism.
- The response asserts that there is “verification [arising from the fact] that the results, for a given candidate, taken through the iVote method align proportionally with results for votes cast through other paper based voting channels”. This is simply incorrect. The results for particular candidates via iVote do not always align proportionally with results for votes cast through paper-based voting channels. In the Legislative Council, the Australian Labor Party, the Animal Justice Party and the No Land Tax party all showed markedly different results via iVote than via other channels. These discrepancies are unexplained.
- There was “post-election audit of logs”. As the described attacks involved interception, spoofing, misdirection, and so on, the anomalies would not be reflected in the logs.

The Response notes that Dr Teague is an advisory board member of Verified Voting, a not-for-profit organisation that advocates the need for elections (paper or electronic) to be reliable and verifiable. Verified Voting regards current electronic voting technologies as not yet sufficiently trustworthy for deployment on the Internet; note that this does not prevent their deployment in voting booths. Verified Voting is a non-partisan organization working for accuracy, integrity, and verifiability of elections. We are proud of Dr Teague’s unfunded advisory board membership of Verified Voting, an organisation that also includes Bruce Schneier, Ron Rivest, and Ed Felten among its directors and advisors; these are scientists of major international standing.

The Response accuses Dr Teague of in some instances failing to declare her association with Verified Voting. This information is clearly listed on her web page and, where relevant, with her publications. But is it not clear why this affiliation is regarded by NSWEC as a conflict of interest. Given that the purpose of Verified Voting is to use robust evidence to ensure that elections are undertaken to a high standard, Dr Teague’s affiliation with Verified Voting doesn’t undermine the value of her arguments, but enhances it.

More generally, the Response makes a range of allegations concerning Dr Teague’s motivation and approach to the issue. She is described at various points in the response in emotive terms such as “anti-”
or an “activist”, and as engaged in disruption of elections – an extraordinarily serious allegation. Some of the allegations are illogical; for example, where a system has a discovered vulnerability it is reasonable for researchers to argue that the public should not have confidence in it; it is not clear why Dr Teague’s demonstration of the existence of flaws in a system that is supposed to be robust is poor behaviour. We believe that her work is undertaken to the highest academic standards, and in exposing this very real risk to the integrity of the NSW election she has performed a significant public good, not an activity that requires condemnation, no matter how embarrassing it is to NSWEC.

Overall, the Response raises questions about the approach being taken by the NSWEC to electronic voting. In addition to the one-sided view of Dr Teague’s work presented throughout, the Response states that “the [NSWEC] view is that internet voting is not a problem for academic cryptographers to solve, but rather an evolving technology requiring a broad range of technical and electoral skills and engagement with electoral stakeholders”. It appears that the NSWEC view is, therefore, that we should disregard the opinion of senior experts in the field, even when, as in this case, there is agreement that the technology is flawed. In general, our society does not endorse deployment of unsafe technologies, even when they have potential benefits, and we endorse the work of researchers who uncover threats to our systems and infrastructure.

Regrettably, the behaviour of NSWEC in this matter does not seem professional. As quoted earlier, the Response was described to us by Mr Brightwell as in part a document that “spells out our concerns with Vanessa’s conduct”. Mr Brightwell, however, has previously received explicit rebuttal of his concerns about her conduct: some months ago he made a formal complaint to the University about Dr Teague, which led to an internal investigation. This investigation supported Dr Teague’s actions. To repeat these allegations about her “conduct” in a public forum, when they have been rebutted both by the University and by independent scientific colleagues of Dr Teague, is an extraordinary act. In their communications with myself and others regarding Dr Teague’s activities, the NSWEC appear to have been selective in choice of evidence, misrepresented the work, not taken proper care to provide context, and shown bias in presentation of Dr Teague’s activities; and in so doing have constructed a view of the work that is unfavorable and unrepresentative. The NSWEC appears to be using its public website as a platform for a personal attack.

We stand by Dr Teague’s view: there is neither evidence that the vulnerability was exploited, nor evidence that it was not. The lack of evidence means that it is indeed the case that confidence in iVote should be low, and the work of Dr Teague in discovering and reporting this vulnerability is fully justified. We believe the NSWEC should repudiate the response, or at the very least post a link to this rejoinder on the Commission’s website to afford the University the courtesy a right of reply; the Commission should have nothing to fear (as we do not) by taking steps to ensure that this discourse is balanced.

Justin Zobel
Head, Department of Computing & Information Systems
University of Melbourne
13 October 2015