CORRECTED EVIDENCE

ELECTORAL MATTERS COMMITTEE

Inquiry into the future of Victoria's electoral administration

Melbourne — 14 March 2013

Members

Mr B. Finn	Mr L. Tarlamis
Ms D. Ryall	Mrs H. Victoria
Mr A. Somyurek	

Chair: Mr B. Finn
Deputy Chair: Mr A. Somyurek

Staff

Executive Officer: Mr M. Roberts
Research Officer: Mr N. Reader

Witness

Dr V. Teague, research fellow, University of Melbourne.

The CHAIR — Welcome to the public hearings of the Electoral Matters Committee inquiry into the future of Victoria's electoral administration and matters related thereto. All evidence taken at this hearing is protected by parliamentary privilege, as provided by the Constitution Act 1975, and further subject to the provisions of the Parliamentary Committees Act 2003, the Defamation Act 2005 and, where applicable, the provisions of reciprocal legislation in other Australian states and territories. I also wish to advise that any comments you make outside the hearing may not be afforded such privilege. Could I ask you whether you have read the *Guide to Giving Evidence at a Public Hearing* pamphlet that the committee provided?

Dr TEAGUE — Yes.

The CHAIR — That is marvellous. I ask you now to state your full name and business address and whether you are attending representing an organisation, and if so, what position you hold in that organisation.

Dr TEAGUE — I am Vanessa Teague. I work at the University of Melbourne. I am endorsed as the expert on this issue by the Computing, Research and Education Association of Australasia. My postal address is the department of computing and information systems in Parkville.

The CHAIR — Thank you very much. I should point out first of all that the evidence will be taken down and become public evidence at some stage in the not-too-distant future. I ask you to begin by making a verbal submission, and then we will open it up to questions at the conclusion of your submission.

Dr TEAGUE — My submission is about electronic voting. Computers are inherently very difficult to observe. You might be able to see what is printed on the screen, but a person cannot tell directly what is actually happening to the electronic data, which is really the fundamental problem about computerising voting. Over the last few months there has been a growing news story about Chinese people hacking into and infiltrating a large number of supposedly highly secured but not highly secured enough sites on the internet. There is absolutely no reason to believe electronic voting systems would be immune. In fact there is every reason to expect that deliberate hacking, manipulation or even just accidental software errors or bugs could potentially cause votes to be misrecorded or privacy to be exposed.

I think there are two important directions behind doing a good job of electronic voting. The first is transparency of the process, which has been controversial elsewhere in the nation but does not seem to be controversial here. I think the source code and the maximum amount of documentation for an electronic voting system should be publicly available. My understanding is that VEC agrees, so I do not think there is a controversy there. Transparency is good for security because the more details that are available about system, the more it can be scrutinised.

Of course that does not guarantee that it is going to be perfectly secure, which brings me to the next main point, which is about verifiability. Verifiability means giving voters evidence that their vote is recorded in the way that they intended without their having to trust that the system is working perfectly. It also means giving observers and scrutineers some evidence that all of the votes are accurately input and accurately tallied.

I have been working on Prêt à Voter with the VEC on a voluntary basis. In fact I worked on Prêt à Voter for years before it got adopted by the VEC. The reason the system is nice is that it provides a complete trail of evidence from the point where the voter looks at their printout and checks that that is the vote they wanted to cast all the way through to the point where a collection of anonymous votes is put out at the other end of the system. It is more complex than alternative methods, but that is because it solves a problem that alternative methods do not solve — namely, the problem of producing evidence that the votes have been correctly transferred electronically without reliance on a secured trail of paper votes that has been posted back or sent back to the counting place. However, it only works as an attendance voting system; it does not work over the internet.

Internet voting is extremely difficult to secure adequately in a verifiable fashion. There are two big unsolved problems. One is authenticating the voters, meaning making sure that the person at the other end of the internet connection is the eligible voter you think they are. The second thing that is hard is providing the voter with evidence that their vote has been cast in the way that they intended. There is really no method of doing that that is secure and still usable by ordinary voters. I can see that there is a big demand for internet voting. I understand that it is accessible and convenient and that it is very popular in the places it has been deployed, but the truth is that there is currently no usable and privacy-preserving way to provide voters with evidence that the system has defended against external or internal efforts to manipulate the votes.

I did read the submissions from Everyone Counts and the New South Wales Electoral Commission, and I am not going to go through and respond to them in great detail, although I am very tempted. But I would like to address one issue that came up in the Everyone Counts submission, and that is the idea that Everyone Counts, as an organisation, has experience in deploying and implementing electronic voting systems and that the VEC does not. I think it is important to understand that the person who actually has the experience of designing, implementing and deploying the Everyone Counts system is Craig Burton, who now heads the project at the VEC. I am not aware during Craig's time as the technical head of Everyone Counts of any incidents of letters showing up in the boxes where the preference numbers were supposed to go. I think that when we are talking about people and their experience of designing and deploying electronic voting systems, the VEC now has superior experience in the form of Craig compared to what Everyone Counts has.

In summary, technology changes very fast. Nobody can say with confidence what technology we are going to be using for voting 30 years from now, but I think the principles of transparent electoral administration and verifiably correct election outcomes stay basically constant, regardless of what technology we are using. I think the Prêt à Voter project is going in the right direction.

The CHAIR — Thank you very much. I think you have made your position very clear. One question I have is concerning your very grave doubts about electronic voting. The thing that immediately jumped into my mind was the ballot draw, which is conducted by the VEC via a computer. We press a button, it all goes bang and out comes the ballot draw. Is that protected in a way that you are not referring to, or is that open to the same sorts of abuses that you are suggesting for other forms of electronic voting?

Dr TEAGUE — You are talking about drawing the candidate order on the ballots?

The CHAIR — Yes.

Dr TEAGUE — I actually did not even know they did that electronically, sorry.

The CHAIR — The AEC still maintains the balls, but my clear recollection — and you might be able to help me on this — is that the VEC conducts the ballot draw on a computer. They press a button, and half a second later you are told whether you are bottom, top or in the middle. I am now concerned, having heard what you have said, that the process might be open to some form of abuse that would not be good for the system.

Mr TARLAMIS — I think from memory they basically type the names into an Excel spreadsheet, then hit a button and it supposedly randomly orders them. I do not know how that actually works, but I have seen them do it.

Dr TEAGUE — That is really interesting. I had never thought about that before or even realised that they do it. There are certainly ways that you could use cryptography to do it in a way that everybody injected a bit of randomness into the process. You could all be standing around — —

How can I explain this? The trouble with a stand-alone computer is that you do not know who generated the randomness that goes into making the draw. There are ways that you could use cryptography to make sure that you could all input some randomness into the process, so you could be confident that it had been properly shaken up. That did not really quite answer your question, which was much more specific. You asked if I thought it was open to abuse.

Ms RYALL — It is probably something that we need to ask them.

The CHAIR — Yes, I think we have something to talk about at 11 o'clock today.

Mr SOMYUREK — You can take it on notice if you like.

The CHAIR — I think it is a really important issue, particularly if somebody is on a slender margin. It could decide whether they remain in Parliament or not. If a ballot draw was improperly interfered with, then you would have to be concerned that other things might be as well.

Dr TEAGUE — I think you are probably right. I think it comes under the same sort of category, but I would have to go back and understand exactly what it is that they do and understand how it could be done better.

Mr SOMYUREK — Yes, it is probably fair that you take it on notice.

The CHAIR — We are certainly very keen to get your view on this, having given it consideration, because it is a fairly important matter that you have raised.

Ms RYALL — I know we discussed this at our last public hearings. If I can summarise what I think you have indicated, it is that we can look at the integrity processes and verification processes; there are ways to do that and do it well; but it would need to be limited to at the booth and not be through an internet-based system. Is that what you are saying?

Dr TEAGUE — That is right.

Mr TARLAMIS — In terms of the security of the electronic voting kiosks in Victoria, are you satisfied that the security is sufficient with those currently?

Dr TEAGUE — I have been working on a voluntary basis on the project that is designing the next round, based on Prêt à Voter. I guess there are two answers to that. One is that there is a process, which I do not really know very much about, for securing the actual boxes, but more importantly there is a process for the voter to look at the vote that comes out of the box and see whether that is the vote they intended to cast.

The argument is that even if the box itself is not perfectly secured, the voter gets the opportunity to directly check that the vote that came out is the right one. The reason I think that is the right way to go is that it is impossible to perfectly secure that kind of a box; you cannot. You are going to have it sitting in an early voting centre for three weeks and somebody has to come in and vacuum the voting centre. You cannot possibly expect it to be perfectly under observation all the time from the point where it gets produced in China to the point where it is voted on. So the verifiability step obviates the need to have a perfect process for securing the box.

Ms RYALL — Given that situation, you would then need to make sure that there was a failsafe system to recast it if the person said, 'That is not how I voted', but that would then pose a problem as to the integrity of the system in the first place, would it not?

Dr TEAGUE — Yes, definitely. I think if something comes out of the box and it is not what the voter wanted, we definitely have to think hard about what to do at that point. Clearly some voters will have just changed their mind or accidentally pressed the wrong button or something; that is going to happen at some rate. It becomes a little bit fuzzy. At what point do you say — —

Ms RYALL — It was their problem.

Dr TEAGUE — 'We've had so many complaints from this machine that we really doubt whether this machine is okay' versus 'We've had this acceptable baseline of complaints'. Are you the person who used to be an auditor?

Ms RYALL — Yes.

Dr TEAGUE — Yes. It is a hard question because you cannot tell. There is going to be some probability distribution of voters just saying, 'This is wrong', and you cannot tell a spike that is within the bounds of that random distribution conclusively from something that really indicates, 'This machine is completely broken'.

Ms RYALL — Or is there is some systemic issue.

Dr TEAGUE — Yes, 'There is a problem. Right'.

Ms RYALL — And in your experience, or from your knowledge of other jurisdictions or countries that use this system, have any of those sorts of problems crept in?

Dr TEAGUE — There are no other jurisdictions that use something exactly like this. There is experience in the United States with a much more simple idea, where you tell the computer your vote and it prints a voter verifiable paper trial. I am actually not aware of any instances in which something has been found to fail at the point of voting. I think it is more often interpreted as evidence after the fact.

Ms RYALL — I guess if you were able to lodge that verification ballot paper, there would be statistical sampling checks, if you were relying on the electronic data to produce the results rather than the actual checking of the ballot papers?

Dr TEAGUE — Yes, that is what they do in America. They do random samples as an audit of those pieces of paper.

Ms RYALL — Yes.

Dr TEAGUE — So Prêt à Voter does a different thing. It has a cryptographic, fancy computer science process for taking the encrypted printouts and producing an answer. I think the right answer to your question is to say that we would not expect any more than a small number of occasional voters to complain that the vote did not say what they thought it should. We would expect that the norm for the huge majority of voters would be that they would have a look at it and it would be fine. I think anything other than a very small number of people who complained that it did not reflect their intentions would be problematic. It would be the box. So if the thing that the voter has does not match the thing that they asked for, it is because the box — the computer that is sitting in front of them — misbehaved.

Setting a completely rigorous description of exactly when you should say, 'This box has malfunctioned', is hard, but I think in practice the expectation would be that it would happen rarely. The right way to think about it, assuming that it did not happen, which most of the time it would not, is to say that you would have a trail of evidence after the fact that a bunch of voters looked at their printout and then this was the result.

Ms RYALL — And this was the reason it occurred.

Mr SOMYUREK — I hear what you are saying about verifiability and the systems not being foolproof, but there is apparently research — I cannot source it at the moment, but I am sure the committee staff will be able to source it — that shows that people will take up en masse the option of being able to vote with hand devices, smartphones and iPads. What is your view on that?

Dr TEAGUE — Do you mean from a remote location?

Mr SOMYUREK — Yes.

Dr TEAGUE — I agree entirely that there is demand for remote voting, and I can see that it is convenient and accessible and that a lot of people would really like it, but it does not provide the degree of evidence that it gets the right answer that we would need to have.

The CHAIR — I think you have again made your position very clear. In the lead-up to the US election last year, I saw a number of reports of voting machines over there producing results that voters had not intended. I am wondering whether you are familiar with those machines, which I gather are used quite widely in many US states. If so, is there any evidence that you are aware of that they have been used for widespread corruption of the voting process?

Dr TEAGUE — This is a good question. There are certainly a lot of people who would say yes. My impression is that there is a great deal of accidental bad programming, bad software and unreliable stuff. I am not aware of any really solid evidence that conclusively points to conspiracy over incompetence, but there are definitely a lot of things that did not go right.

I think the best example, which is possibly not in my submission to this inquiry but is in a supplementary submission I wrote for the New South Wales equivalent of your inquiry, was a case in Florida in which the little box was misconfigured. It was a touch screen, and when you touched one candidate it reported a vote for the candidate who was actually below them and vice versa. It did have a little paper trail, so they could kind of tell from going and looking at it afterwards that this had happened. I am not quite sure how it did not get picked up at the time, or maybe it did get picked up at the time. I am not exactly sure what happened at the time, but I know that the misconfiguration error caused a wrong output. It caused the wrong election outcome to be announced, and then they went back to the paper trail later. They went back to it, examined it and decided that this had been wrongly configured.

The CHAIR — So any use of electronic machines would have to have some sort of paper trail in your view to verify it.

Dr TEAGUE — I think so, yes.

Mr TARLAMIS — With regard to the iVote system in New South Wales, I think you have spoken to us previously about your views about that. They published a feasibility study that outlined the iVote project and its feasibility in some details. Are you familiar with that? If you are, has it changed your view?

Dr TEAGUE — I have read it, but it was many years ago. That feasibility study long predated the project. I have read it. I cannot remember the specifics.

Mr TARLAMIS — Everyone Counts talks about how it developed this feasibility study report that was tabled in the New South Wales Parliament, but it does not say when or whether it was prior to or after iVote coming in. It does not give that detail.

Dr TEAGUE — It was long ago in the early stages when they were just thinking about it, so it is quite an old document now.

Mr TARLAMIS — I was not sure whether it was a report that had been commissioned afterwards to see whether it had been effective after it had been implemented.

Dr TEAGUE — There were reports that were produced after it had been implemented. That is how I know that there were letters in the boxes where the preference numbers were supposed to go. I think last time I was here I mentioned some of the things that came out of those reports afterwards that said quite negative things about its security and its reliability. I am not quite sure why Everyone Counts has referred to the feasibility study in its submission, because that came long prior to the project.

The CHAIR — Thank you very much indeed. That is most informative, and you have given us an enormous amount of food for thought, I can assure you. The transcript of this evidence will reach you in about a fortnight. You can check it for typing errors, not that there will be any typing errors, I am sure. If there are any typing errors, you can point those out. If you could resist the temptation to change anything else, that would be a marvellous thing. Thank you very much. We do appreciate it.

Witness withdrew.