T R A N S C R I P T

ELECTORAL MATTERS COMMITTEE

Inquiry into electronic voting

Melbourne — 24 October 2016

Members

Ms Louise Asher — Chair
Ms Ros Spence — Deputy Chair
Ms Lizzie Blandthorn
Mr Martin Dixon
Mr Russell Northe
Ms Fiona Patten
Mr Adem Somyurek

Staff

Executive officer: Mr Mark Roberts

Witness

Mr Ralph McKay, founder, BigPulse.com *(via teleconference)*.

Necessary corrections to be notified to executive officer of committee

The CHAIR — Thank you Mr McKay. We are doing a small number of public hearings today. Before we start can I check that you have read the giving evidence at a public hearing pamphlet that was provided to you?

Mr McKAY — Yes, I have.

The CHAIR — So do you fully understand the issue of privilege, which you can have through this forum but not in other forums?

Mr McKAY — Yes.

The CHAIR — Thank you very much for the very comprehensive submission that you have provided to the committee. Can I ask you to perhaps give a couple of introductory comments to it. We have allocated 20 minutes for you. Before you make your introductory comments could you please state your full name and your business address and advise the committee whether you are attending in a private capacity or you are representing your organisation officially.

Mr McKAY — Yes, thank you for the invitation to provide evidence. Ralph McKay, founder of online technology company BigPulse.com. I am representing BigPulse, with a business address located at Newport, New South Wales.

The CHAIR — Please proceed.

Mr McKAY — I am a practitioner with 16 years continuous responsibility for the development of the BigPulse voting technology as well as management responsibility for many thousands of online elections in many countries. These have all been non-government elections and virtually all to a higher standard of vote security than seen in the few government elections to date that have used online voting.

I am frequently asked by new clients, particularly by many universities and IT groups, 'How can we be sure that the online election result from BigPulse can be trusted?'. My answer never fails to satisfy — that is, after voting closes, you have the ability to publish all counted vote receipts and then invite everyone to locate their vote receipt in the counted list. That is a fully transparent vote audit. This technique allows anyone to perform or initiate an independent count, because everyone has convenient access to all votes counted. Now, this response satisfies all because it leaves nothing in the election result to trust. It is practical, non-technical and easy to understand. A verification process that removes the need for blind trust in the black box technology quickly earns greater trust. The same verification process is commonly used by clients in rigorous prelaunch testing.

It is interesting that this long-established gold standard in verifying the fairness of electronic elections is not a feature of the submissions to this hearing in favour of iVote. I have not seen it mentioned. The technique was not employed by iVote in the New South Wales 2015 state election, so I believe it is very important that the Electoral Matters Committee explores why iVote is not offering a transparent audit to dispel all doubts about the fairness of the votes counted. It does suggest a lack of confidence in what may be seen. Chair, I have more to say on this and I am happy to go on, but I will just ask whether you would like me to.

The CHAIR — I think I would like to give the members of the committee a chance to ask you some questions. Again, can I indicate that the committee is going to New South Wales to talk with the electoral commission about iVote. I have taken note of your question; I am sure we will ask a range of them.

Ms PATTEN — Thank you, Ralph. It is a very interesting submission that you have presented to us. Can I just get an understanding: I think one of the main components of your testimony is that we should not be considering electronic voting at this stage.

Mr McKAY — I have not absolutely said that, and maybe it has a place for local government. Particularly what I am saying is that if it is going to be used, really the precondition is a readiness to accept a failure. I say that because one thing everyone agrees on is that there is no way to guarantee that the correct votes are actually recorded on the central server. The verification process is critical, and therefore my point is that it needs to be an absolutely secure verification process and, when that is the case and because no-one can guarantee the correct votes have arrived, it means that sometimes it is going to show a failure, and it is that unwillingness — that fear of disclosing a failure — that is the reason for not using a transparent audit, in my opinion.

Ms PATTEN — I appreciate what you are saying there, Ralph. Obviously we have failures in our offline system. Just looking at the recent media with the number of people who got ticked off the electoral role twice shows a failure in the system, as well as people who have unintendedly voted informally. We accept those failures, so is there a point at which we could accept a level of failure in electronic, or because it is electronic we will not accept anything except for something that is 100 per cent?

Mr McKAY — I agree with submissions from some other groups that make the point that really it should be at least as secure as the current paper vote system. I guess that allows for some error, but the clear risk is that it is much easier for a systemic system-wide error to be introduced with an electronic system. It makes it much more important for there to be a transparent, secure audit of the process. It is that old problem: you cannot put the toothpaste back into the tube once it is out. Elections cannot afford to fail. It is a core thing with our democracy. If the election is re-run, is it going to get the same result as it should have the first time? I am not attempting to express a strong opinion on those points, but that is what needs to be carefully considered.

The CHAIR — In your submission you have singled out one particular category of people. These are people who are victims of domestic violence, where you say that the coercer can find out if the person being coerced has changed their vote, and you highlight this as the fundamental flaw of the New South Wales iVote system. Have I read your submission correctly?

Mr McKAY — Yes.

The CHAIR — I just want to know: is your objection based solely on this category of person?

Mr McKAY — It is a very fundamental point. If coercion is not managed, why have a secret ballot? If coercion is managed, the way it is managed is with a revote. If we are going to allow people to revote, obviously the revoter, the coerced person, is normally expecting that the act of revoting will remain secret. This is a special case where not only the elector's ballot preferences must be kept confidential, but also the act of revoting. It is a double secret.

The problem I have with iVote is that it is not protecting the secret, but it does it in a way that it still defeats the coercer, because it is not until after the election has closed that the voter gets a chance to find out if the vote was counted or not. If it was not counted, if they trust the system, they will correctly assume that it is because they were tricked with a secret revote. So the idea works by keeping in the dark, not disclosing to the vulnerable elector that is being coerced and revoting, that their secret is not going to be protected. That is the bit that disturbs me most.

This is the problem. This is the very reason why electronic remote online voting is a difficult issue with government elections, because this is where coercion really matters. You are trying to manage it. The very process of managing coercion clashes with the need to verify the election with a transparent audit. The transparent audit allows anyone to see which votes were counted and therefore if any revotes were used to defeat coercers. It is not an easy point to understand, but it is the fundamental point.

The CHAIR — Okay. I just wanted to check that that was your fundamental point.

Mr DIXON — Thanks, Ralph. Your verification method where you said to people that it dispels all the worries is that you can actually check that your vote is physically there. How would one do that? Does the receipt that is printed out have an identifier on it that the voter knows? How does it actually work?

Mr McKAY — A very high quality vote receipt is a precondition for a transparent audit. iVote does not have a high-quality vote receipt, so it could not have a transparent audit currently anyway. But as long as the elector cannot easily make a false claim about what the receipt is showing, then all the elector has to do is visit a web page which displays a list of all vote receipts — that is, each vote is given a unique code, and using a search they can locate their personal receipt and then feel confident that it is in fact counted. Now, there are subtle ways to trick even this system. I do not think this is probably the place to go into it, but there are also remedies. There are traps in the transparent audit as well; that is what I am saying, but they can be overcome. But it is certainly the gold standard.

The CHAIR — You explained that you were not successful in the tendering process for New South Wales iVote, and I am trying to put this with some subtlety and discretion — —

Mr McKAY — Agree.

The CHAIR — Would it be reasonable of me to say that because you were an aggrieved party you will therefore have criticisms of the New South Wales iVote system, or would it be incorrect to say that?

Mr McKAY — I think all my comments are factual. It is actually not motivated by whether we did or did not win the tender. I have certainly made the point that the tender was an unfair process. We were not invited into the tender; that was really what our complaint was. We were eliminated after expressing interest, and we received an unsatisfactory reason for why. I feel it is related to the fact that we would not allow our technology to be used in a government election unless we were satisfied that it was being used at the correct standard, and I am yet to know how these intractable issues could be solved.

The CHAIR — Can I also ask, in the absence of any questions from my colleagues — —

Ms PATTEN — I have one after you.

The CHAIR — Fiona will follow me. I am interested that you think that it is all right if a local government election fails but it is not all right if a state government or federal government election fails. I have never been a member of a local council, so I do not particularly have a view on that, but could you just explain the rationale for why it does not matter? I am assuming if a university election fails, you are fine with that, or if my football club's election fails, which is electronic, you are fine with that, but is it allowable for local government to fail? If you could just give me the rationale for that.

Mr McKAY — No, I have not said that. I do not think it is acceptable for any election to fail. I think in the submission I said the word 'perhaps'.

Ms PATTEN — Is that a scale thing — that you have smaller numbers in the wards and the councils?

Mr McKAY — Clearly it is more significant if a federal election fails than local government. That is really the only point I am making. I am not suggesting that it is okay to fail at any level.

The other point that is relevant here is that the reason an election is likely to fail at a government level is because of the motivation for an attack. There is a much higher motive for election criminals or foreign-based cyber armies to interfere with the result. So there is a risk trade-off there. With the sorts of elections that BigPulse operates in, that risk really does not exist. We have other sorts of risks. Certainly with hackers we have the same sorts of risks, but we have managed to protect ourselves from those risks.

Mr DIXON — Have you been hacked?

Mr McKAY — No, not to our knowledge. We have not been hacked. We have never had any security breach that we have had to be concerned about.

Ms PATTEN — Just one final one to help us with our questions to the electoral commission in New South Wales: when we are talking about people verifying and then revoting, you stated that you think that that was because they were coerced — that they have instructed a revote. When we have considered it we have thought that people might just change their mind and revote, which the New South Wales system allows. I just wonder if you can comment on why you put it down to coercion rather than a change in policy ideas or new information.

Mr McKAY — The New South Wales Electoral Commission has made it clear in its security implementation statement, released before the 2015 state election, that the system contains an anti-coercion mechanism, so it is attempting to manage coercion. The point about revoting is that you do not know for sure why someone is revoting. If they are revoting because they are feeling coerced, they may not be telling anyone that is the reason. The point is: if it is being offered, it is reasonable to assume that someone may want to use it and therefore there is an obligation to protect the interests of all those who are using it.

Ms PATTEN — We have talked about this. Postal votes are open to coercion, obviously, for exactly the same reasons.

Mr McKAY — Yes, but the postal vote does not pretend to offer a remedy.

Ms PATTEN — Okay. I see.

Mr McKAY — It accepts the risk. iVote pretends to offer a remedy, and it does in fact work but it has an expense. The way I put it is that it is breaching the trust of the revoter. To my way of thinking it is totally unacceptable. It is a form of quackery.

The CHAIR — Thank you very much, Mr McKay, for your very, very comprehensive submission. I think you have probably given us a lot of food for thought. It is probably just as well that we have taken your evidence in advance of going to our meeting with the New South Wales Electoral Commission.

Can I also advise you that this has been recorded by Hansard and that you will receive a transcript within a fortnight or so. You cannot change your evidence, but if you think there is an error of fact or something like that, feel free to send in any amendments that you consider to be important. So thank you very, very much.

Mr McKAY — Chair, may I make one 30-second final comment?

The CHAIR — Yes, you may.

Mr McKAY — In my view the most important statistic to ask for in the iVote experiment is the number of people who requested a revote and the number who actually revoted —

The CHAIR — It is 1.7 per cent.

Mr McKAY — because revoting was offered as the remedy for anyone who suspected vote corruption or who felt coerced. These two critical revoting numbers have not been released.

The CHAIR — So where does your 1.7 per cent figure come from? I see, you wrote 'apparently just 1.7'.

Mr McKAY — I believe that is the number of people who attempted to verify their vote; that is not the number of people who actually revoted. Now, the revoting number to me is the central statistic in measuring the performance of the system.

The CHAIR — Thank you very much for that piece of advice, and again thank you for your willingness to participate in this inquiry.

Mr McKAY — My pleasure. Thank you.

The CHAIR — That is the end of the public hearing for today. The meeting is concluded.

Committee adjourned.