T R A N S C R I P T

ELECTORAL MATTERS COMMITTEE

Inquiry into electronic voting

Melbourne — 22 August 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
Research officer: Mr Nathaniel Reader

Witness

Dr Roland Wen.

Necessary corrections to be notified to executive officer of committee

The CHAIR — Thank you, Dr Wen, for coming along to these public hearings of the Electoral Matters Committees and for putting your effort into doing your submission and for being present today. I just want to check with you, please, that you have received your copy of the guide to giving evidence at a public hearing pamphlet.

Dr WEN — Yes, I have.

The CHAIR — You have. Obviously you would understand, then, that this committee has parliamentary privilege, but anything said outside does not have parliamentary privilege. Could I please ask you to state your full name and your business address and to advise the committee whether you are attending in a private capacity or whether you are representing an organisation. Then feel free, if you would like, to make some introductory comments, and then we will ask questions. Again I apologise for keeping you late, but we had a couple of additional questions to the previous witness.

Dr WEN — My name is Roland Wen. I am from the University of New South Wales, the school of computer science and engineering. I am appearing in a private capacity.

Thanks for the opportunity to be here today. It is a really timely inquiry because there is this move towards e-voting that has been considered around the world, and national and international experience so far has revealed that there are many, many issues to consider. These can be broadly broken down into four categories of issues. The first three categories are covered in other submissions that have been made, so I am just going to touch on them briefly. But the fourth category, which has not been well addressed anywhere in the world, is that we need to carefully plan how to actually build an e-voting system as a piece of critical national infrastructure, and I am going to spend most of my time on that.

The four categories are: one, issues about weighing up the risks and the benefits of e-voting; two, issues about the vexing question of deciding between internet voting or polling place e-voting; three, issues about transparency, scrutiny and trust; and four, as I have mentioned, issues about how to build an e-voting system so that it is fit for purpose as critical national infrastructure.

I will start with the first category of issues, which is weighing up risks and benefits. Now obviously in considering whether to use e-voting the first thing that is needed is to understand what the risks and benefits are, but the thing to notice is that all the risks have not yet been identified. This is not surprising because it is so new and it is just not well understood. It is very easy to overlook risks, especially because there are so many subtle ways to attack electronic systems. For example, an attacker could compromise the secret ballot on a large scale by collecting metadata from different electronic systems to potentially identify voters and how they voted. This is one of the risks that is really commonly overlooked. A lot of careful thought and analysis is needed to understand the risks. This inquiry is an important first step, but there is a lot more work that needs to be done.

The second category of issues is resolving the vexed question of internet voting or polling place e-voting. Now pure internet voting is much riskier than pure offline polling place e-voting because internet voting has all these additional risks such as the loss of the secret ballot and the lack of control over voting devices. But most of the risks of internet voting are still shared with polling place e-voting. In fact in practice many polling place e-voting systems do have online components, so they are not pure offline systems. So these online components are potentially vulnerable to large-scale remote attacks. For example, this was the case for the vVote system, where the voting devices were online. So if, say, the decision is made to go with polling place e-voting to avoid these sorts of online risks, then we have to be really careful not to inadvertently reintroduce those risks.

The third category of issues is transparency, scrutiny and trust. What we really need is new approaches to transparency, scrutiny and trust that are specifically designed for e-voting and electronic systems as opposed to the manual processes that we have now. Many different issues will arise, and things like verifiability and publishing the source code can address some of these issues. But the fundamental issues still need to be addressed of scrutinising the quality and security of e-voting systems to ensure that they actually prevent failures and attacks. This requires a lot of thought and planning well in advance.

The fourth and final category of issues is building e-voting systems as critical national infrastructure. We can see from the recent census failures that it is clear that that system was very much commercial grade and operated in a commercial environment where the risks were not managed, so it is really pure luck whether something goes wrong or not. In that case things went terribly wrong. The key point I want to make is the importance of building e-voting systems using failure-critical engineering practices to manage these risks. This is where most e-voting systems have been let down. E-voting systems previously used in Australia and worldwide are commercial grade or worse, but they really need to be failure-critical grade and to provide very strong assurance of their quality and security. In a commercial environment we see that compromises and shortcuts are frequently made due to resourcing and time pressures, so you have things like testing only happening at the end, reviews and audits are just not carried out, risks are not continually assessed, and there is a focus on compliance rather than genuine security. These sorts of things happen all the time, and it is just completely inappropriate for it to happen in e-voting.

We need to work out what is the most appropriate way to build e-voting systems, and it is a very difficult problem because the expertise in the IT industry at large is in building commercial systems. In our submission we said that electoral commissions need to build up technical expertise and capabilities, and this is a really important thing to do. But at the same time, failure-critical engineering needs a broad range of very highly specialised expertise, and it does seem impractical to expect electoral commissions to have all of this expertise to build critical national infrastructure. Really that was the underlying problem with the ABS and the census failures.

Perhaps the bigger question is: who should build e-voting systems? A model to consider is a separate organisation that has this responsibility as a sort of partnership with representatives from electoral commissions, the Department of Defence, who all work together with a range of experts in failure-critical systems and security. This would be a significant change, but it is worth exploring as a way forward. These are the four categories of issues, and I welcome any questions.

Ms SPENCE — I have what seems to me almost a simple question: based on all of that, do you believe that it is possible to have a system that is secure, verifiable — all of the criteria that have been listed?

Ms PATTEN — Failure-critical engineering.

Dr WEN — There are well-established ways to develop military-grade systems and aeronautics. There are a lot of engineering practices to provide high assurance of quality and security of systems, but whether we can guarantee that these systems will be completely secure — no. There is always going to be some sort of risk. It is about how we manage the risks and understand the risks and whether the risks are acceptable at the end of the day.

Mr DIXON — Just in a very practical sense, having a polling place and having electronic voting happening there, is it an incredible cost? You have got an election every four years, for example, so you have got to take all the equipment. Has it got to be upgraded? Just all the mechanics and the practicalities of that — it is going to cost a lot more, I would presume, in the long run.

Dr WEN — Yes, absolutely. Often technology is seen as a way to reduce costs, but in reality, if you want to do it well, the costs can potentially increase a lot. I suspect it will be much more expensive to do it well — definitely more expensive than it is now with the electronic voting systems that we have around the world.

Ms BLANDTHORN — Recommendation 3, where you say a single national approach to e-voting should be considered, do you think that that is a whole system that should be rolled out, or do you think that a particular part of the voting process — say, counting or casting a ballot or whatever, a smaller part of the process — should be perhaps, even if nationally rolled out, considered first? Or do you think the whole system should be developing together?

Dr WEN — I think doing things gradually is a good way to do it. If a national approach were to be taken, it is a very big change and it is not something we can roll out on a very large scale all at once. Yes, definitely it is worth doing in pieces, and especially — —

Ms BLANDTHORN — Is there a piece that you think is easier or should be done first?

Dr WEN — To see things that are in common — for example, things like electronic rolls are things that, I think, a lot of electoral commissions each sort of have their own system. Potentially, yes, there can be collaboration on that, and there can be a lot that can be learnt in that process of collaborating.

Ms PATTEN — In this you looked at our vVote system in Victoria, and I think at the end of the day you sort of said it did not work, really. What were the main criticisms of that? Was it obviously probably not to the failure-critical level that you would expect us to be at? Could you give me some examples or specifics of where you saw it failing?

Dr WEN — In terms of the resourcing for the project, it was largely a volunteer research project rather than a serious engineering effort. So there were very limited resources in practice, and lots of things that needed to be done were not able to be done, even basic things like writing up documentation, the software implementation. There was one person responsible for developing the bulk of the system, and that is not what you want. Even for a commercial system you would want a team so that you could have good engineering practices. I think it was a matter of resources to a large extent, yes.

Ms PATTEN — If we were going to build failure-critical infrastructure — and I can understand why you would want to do that at a national level — if we started now, how long do you think it would take us to be able to implement even the first tranche of such a change?

Dr WEN — It is really difficult to give some sort of estimate because it does depend a lot on organisational culture and management, and that is something that takes a long time to change. It is good to start now and start early, but realistically it is a time frame of years that we are looking at.

Mr DIXON — Just on that, I think there is a willingness of the customers to want to accept it. You do not have to educate people; I think they are ready. They are ahead of everyone else, in a way.

Ms PATTEN — That is right.

Dr WEN — That is right, yes.

Ms BLANDTHORN — You mentioned before that it would never be without risk. Is there a level of risk that you think, within this type of field and in your experience, would be acceptable? Do you have a view about what level of risk, if we were to consider it, we would have to accept or should accept?

Dr WEN — In terms of level of risk, it is specific. There are lots of different risks with different issues, so it depends on what sorts of risks are considered acceptable. For example, with internet voting there is no more secret ballot, so that is a significant risk. Is that acceptable? There may be certain benefits for certain groups of voters where it may be considered that the risk is acceptable, but there is no sort of single-level, across-the-board, 'Yes, we can accept this risk or no'. It is very context based.

The CHAIR — I am actually seeking — you will have to put it in layman's terms for me — your technical advice. I have read what other submissions have suggested, but I would like you to answer my question if it is possible for you to answer it. Why can I give my credit card number to an airline authority and have every confidence that the card is fine? Why can I transfer all sorts of money between my bank accounts and pay various bills and put money into Qantas Cash? I am probably not meant to be plugging one thing, but at any rate why can I do all of that and feel very, very confident and have never had any abuse of that, and yet so many of these submissions — and yours is one — are telling me: do not do internet voting. As I said, I have read why other submissions can answer the question, but I am actually interested in your knowledgeable explanation of why the two are so different.

Dr WEN — It is a very common question. Really there are two main points. One is that e-systems are not secure, even though banks and whatever spend billions of dollars on security. There is a lot of credit card fraud, there is a lot of fraud with online banking and the systems do fail. You see national outages of the ATM network every few months in the news. A lot of this is about cost benefit with banks. If you use a

credit card, banks make money out of it. They want it to be as convenient as possible. They are willing to wear some of the cost of fraud.

The second point is that banking is just completely different from voting in terms of secrecy. It is the secret ballot that makes voting such a difficult problem. It is kind of like doing online banking or any sort of banking in total secret, where you have no verification of any transactions; you do not get any account statements to check your transactions. Would you trust the system then? Everything is anonymous as well, of course, so that is a good thing to compare. Would you trust banking in that case?

Mr SOMYUREK — I think the point is, a month ago for the first time I had $4000 disappear from my account in a transaction I did. It did not get to the recipient. I do not know what happened to it. There was an investigation, and there was a remedy for my situation: the bank gave my $4000 back to me. But with the vote there is no remedy. That is ultimately the bottom line, isn't it, really?

Dr WEN — Yes, that is right. The banks want you to have confidence in the system, and they will give you your money back if you are a victim of fraud. But you cannot do that with voting.

The CHAIR — Any further questions? Again, thank you very much for your willingness to provide so much in your submission and today. You will receive a copy of the transcript within a fortnight or so, and you can change any errors but you cannot change wholesale slabs of the transcript to make yourself express something different to what you actually expressed. Again, thank you very, very much. The committee greatly appreciates your time.

Dr WEN — Thanks a lot. It is my pleasure. Thank you.

Witness withdrew.