TRANSCRIPT

ELECTORAL MATTERS COMMITTEE

Inquiry into electronic voting

Melbourne — 24 August 2016

Members

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

Staff

Executive officer: Mr Mark Roberts

Research officer: Mr Nathaniel Reader

Witness

Mr Stephen Wilson, managing director, Lockstep Technologies.

Necessary corrections to be notified to executive officer of committee

The CHAIR — Thank you for appearing before the Electoral Matters Committee and this hearing on electronic voting. Can I just check that you have received your guide to giving evidence at a public hearing?

Mr WILSON — Thank you.

The CHAIR — And that you comprehend that you have parliamentary privilege in this room but you do not have it outside of the room, which might make a difference to what you want to say. Hansard will be recording your evidence. Could I ask you to please state your full name and your business address and to advise the committee as to whether you are representing your organisation or attending in a private capacity. Then you might want to add to your submission.

Mr WILSON — Good. Thank you, Chair. My name is Stephen Wilson. I am the managing director of Lockstep Technologies. Our business address is 11 Minnesota Avenue, Five Dock, New South Wales 2046, and I am appearing as a representative of Lockstep Technologies.

By way of introduction, I am a researcher and adviser in the specialised field of digital identity and privacy. This is a subset of cybersecurity. Of course security weighs high on all of your minds with respect to e-voting. I have been involved with security for 21 years — a lot of electronic government work, a lot of electronic health work and finance work — so I have seen a great spectrum of electronic use cases with differing security requirements. It is a many-splendoured thing.

When it comes to e-voting of course you have probably already heard about the challenges of availability and resilience and software quality, and I notice that the VEC was talking about software quality and verification. We have hacking, we have got fraud and we have also got identity. My research is specifically into identity and anonymity, which is the flipside of identity, and some years ago I produced a peer-reviewed research paper, which I submitted to the inquiry, that explored very particular properties that we think are essential but not sufficient to produce electronic voting.

I want to emphasise that the paper that I submitted and my coverage today are not about a complete solution to electronic voting. It is a hell of a problem. I agree with the witness who said that this is perhaps the biggest challenge in all of software. But I do think that the identity and privacy and anonymity areas have got some new promise through smart technologies.

On that, what interests me is the digital challenge of one person, one vote. I am going to talk about keys, and I think you have already heard about keys. It is a hell of a metaphor. I think that we should have rethought this 30 years ago, but it is too late. A key is essentially a mathematical code or a number which is assigned to somebody and they use that number in software to access something online, or subtly, to leave their mark on something — to authorise a payment transaction or in this case to leave your personal mark on a vote. Keys can be anonymous, and of course with electronic voting they have to be anonymous. When we are talking about keys, the voting problem becomes one person, one key, one vote. This is really tough because we want to have anonymity but we also want to have certainty that the right keys are in the right hands. Of course think about that for a minute and it is really paradoxical. What it appears to call for is a nation-scale identity management system, and I say 'system' — —

Ms PATTEN — You could have said 'card' instead.

Mr WILSON — No. No, this is really important, and I know that there is some awkward laughter about this. But I think that, with respect, you are reflecting the fact that Australia has really struggled with this, and we all know that. So it is really important to be able to talk with precision about identity management systems as opposed to identity systems. A simple parallel is that we have a very consistent way of doing electronic banking and every bank card, regardless of whether it is American Express or Visa or any bank, behaves almost exactly the same. It is very standardised and it is full of security features. But of course no law says that you need to have one person, one bank card, so within that system we have a single banking system but we have many, many different bank accounts. Identity management is like that.

Identity management is a subset of security. There is a whole profession and a practice and an industry around identity management technology. In one of the foils that are provided — really just two foils — the triangle is reflecting a really important shift in the last few years where my colleagues are focusing not so much on who somebody is anymore but what they are. So we are very interested in being able to be precise about people's entitlements, people's different bank accounts, without pigeonholing everybody into one Australia card. Believe it or not the identity industry by and large is against singular identity, not just because they want to sell more tech but because we are all very conscious of privacy. There has been this interesting shift and that triangle in the foil reflects research and development that Lockstep Technologies has done on how to take an entitlement such as registration to vote. The fact is that somebody might appear on the electoral roll; you want to reflect that fact in a key that does nothing more than reflect the fact that somebody is on the electoral roll and then give them the ability to electronically stamp a ballot, leave their mark with the key.

Very quickly I will talk about a kind of a strawman voting system, which was in the paper that I have submitted, and we can now, with the second foil, talk more about how mobile phones — smart phones — could be used. I want you to imagine that one utopian way to do electronic voting would be for the government to issue everybody a special smart card with the number on the front of it. It looks like a payment card, but it has got a number like a voting number, completely random, and a chip. You give that to everybody, and come voting day you would use this thing in a terminal to mark your ballot with that number. The number cannot be linked to your identity because it is just random, and that card would only ever be used once. Thanks to the technology of the chips in the card, the card cannot be counterfeited, it cannot be cloned and your vote cannot be messed with. Just like a chip from a banking transaction, you cannot mess with the ballot once it has been cast. So that sounds pretty good.

The simple fact now is that smart phone technology has got to the point where we have cryptography and we have got keys and we have got the technology built into the silicon chips and the phones such that you could do this with telephones instead of smart cards. That is the kind of infrastructure approach that Lockstep has been involved with. I am just trying to give a sense.

One of the really important policy determinations that I would like to just repeat is that we can now start talking about identity systems and nation-scale identity management systems without getting sucked into that black hole of a single identity. Obviously there are very few e-voting systems at nation scale that appear to be working. One of them is Estonia. People always remark that Estonia has this national ID card that appears to be the cornerstone of their electronic voting. I simply ask people who are exploring the space to abstract away from that and to understand that a uniform way of doing identity — diverse plural identities — is really important and that there is no way the identity management practice that I am a part of would advocate a single identity; it is just not necessary and not sufficient. Even if you had that single identity, it is not obvious that you could vote with it anyway. Thank you.

The CHAIR — Thank you very much for your submission and your willingness to come along.

Ms PATTEN — Thanks, Stephen. So we have the part of being able to verify that the voter is who the voter says they are and the system that you outlined does that. Obviously on top of that we need to ensure that we verify who the voter is, but then we ensure that the voter's vote is anonymous so that it cannot be linked. I take on board that your system does that. Have you looked at the voter verification side of iVote?

Mr WILSON — No, not at the expert level that I would want to give a professional opinion about that.

Ms PATTEN — Okay. I was just interested in if you had any thoughts on that. I guess that is one part, but then obviously we have the other issue of verifying that the vote that the voter placed is the vote that ends up in the ballot box.

Mr WILSON — Yes, and that of course is one of the subtle properties of electronic voting. There is always a list of 10 or 12. I know that some of your submissions have traversed that ground really well. Verification is tough — the receipting of your voting as you walk out of an electronic polling place.

Ms BLANDTHORN — In a system where people had a number or a card, how would you stop them either giving those numbers or cards to other people or coercion to do so?

Mr WILSON — Yes, coercion is another issue. With this sort of system you can show that a vote has been used more than once. That is probably the limit — —

The CHAIR — Because you are giving it to someone else.

Mr WILSON — Indeed, so that is probably the limit of the technology — —

Ms BLANDTHORN — For them to cast even with their first vote.

Mr WILSON — Yes. If we look at a phone instead of a card, modern phones have things like a thumbprint scanner or a biometric in case the phone falls into the wrong hands for any other purpose, like paying. There is almost nothing that you cannot do with a phone these days, so it is important that a phone falling into the wrong hands is safe. That would give some measure of protection against re-using a phone to cast a vote, except for coercion, so you have still got that issue that you might somehow coerce a vote. It would have to be done physically, so that might provide some comfort that you would literally have to strongarm somebody and force them to present their biometric to activate the phone and then vote from that phone.

The CHAIR — I am actually interested in the person who cannot be bothered voting, because I have heard so many excuses over the years, as all MPs have, that 'I've just been fined by the VEC for not voting and this was my reason', and there are a range of reasons which show a disconnect with the political process. But what if somebody said, 'I can't be bothered voting; I'll just give my card to my son to go and post my vote' — —

Mr WILSON — Or sell my vote to somebody else.

The CHAIR — Let us just do 'give'; let us not even move to 'sell'. What if a mother cannot be bothered, she has a million things on her plate, she gives the card to her daughter and says, 'You go down and vote'? Or the way that I would see is a lot of young people saying, 'I don't know how to vote; Mum, you take it; you go down and do it'. What is to stop that under the sort of system that you are putting to us?

Mr WILSON — Across any technology I think there is very little to stop that. I think that is one of the stark differences between e-voting and paper voting — the interface. One of the experts in this area said 10 or 20 years ago that the problem is interfacing the cryptography to the system, meaning how do you stop that cryptographic magic falling into the wrong hands through coercion, or somebody cannot be bothered, or maybe they sell their vote. I think that there is no silver bullet for that in technology; that is tough.

Mr SOMYUREK — Just in terms of voting twice, or more than once, that is not a real big problem in Australia — it does happen, but not often. I would have thought that you could design software so that you cannot vote more than twice on the same card.

Mr WILSON — Yes, that is in the paper. You would show that this key can only ever be used once.

Mr SOMYUREK — So when you say that you might vote multiple times with the cards, you can actually design it so you cannot vote more than once on that card, yes?

Mr WILSON — Yes. I think the question that I was responding to was, 'If you are not going to use your card at all, could you get somebody else to use it?', and you could, once.

Mr SOMYUREK — Right, but not more than once?

Mr WILSON — No, not more than once. This technology can be quite straightforward to prevent more than once.

Mr SOMYUREK — I would assume it would be, yes.

The CHAIR — Thank you so much for coming along and for your willingness to be so frank with us. You will receive a copy of the Hansard transcript in two weeks time. You are at liberty, obviously, if you think there is a factual error, to correct it, but you are not at liberty to change your evidence.

Mr WILSON — Good. Thank you.

Witness withdrew.