Harry Ridgewell: So how secure are e-voting and remote e-voting? And are they any less secure than voting in person or by post?

Steve Schneider: Well they're issues ... When you talk about e-voting and remote e-voting there's different kind of aspects of e-voting. So I would say electronic voting is using electronic equipment to count your vote and also to process votes and produce a tally. And the capture of votes can be done in the polling place so that I would still consider electronic voting but under controlled conditions. And then remote e-voting is more like, I would call internet voting. Voting over the internet. And so they're both flavours of electronic voting.

Steve Schneider: When you say, how secure are they? It's often a particular system. Different systems have different elements of security. You're talking about the principals of electronic voting and how secure is the notion of using electronic equipment in the first place to do voting? Then there are general issues around security in electronic systems to do with say authentication and identity management and then management of the systems themselves so that they can be accessed in unauthorised way where the people that are in control of them can make changes to what's going on so in cyber attacks. Whether you can be confident that the act that corresponds to the inputs.

Steve Schneider: So there are general issues around security in electronic systems generically before you get into [inaudible 00:02:03] that have to be consented in the voting context. I would say where you're talking about voting in person, one of the issues around doing things electronically is that it's a lot less tangible or visible what, how the information is being handled. Or how the data is being handled. So when you vote on paper, people have an idea of how the votes are being handled. And although there are also questions around that, doing things that are less visible because their electronic systems requires different safeguards to be confident of what's going on with the data. And then where you've got systems that can be, that are electronic there can be systematic ways in which they can be attacked. Which on paper systems would require a much larger number of people to work together in terms of being able to attack an election.

Steve Schneider: So there are general issues around electronic systems that mean that security is a concern.

Harry Ridgewell: Are you able to comment on how secure the voting, polling stations used in America are?

Steve Schneider: There are certainly being questions raised about the equipment, the machines that are being used. They use a whole variety of machines. And there are concerns that they are not very secure in the sense that, they could be attacked if somebody was minded to attack them. I haven't seen reports that these things have actually been attacked in live elections. There was a security conference a year ago that brought a number of these machines into the conference. The E-Voting Village I think it was called. Where various attacks were demonstrated to

be possible on these machines. So that was in the context of a security conference. But the machines were the machines and it was shown that it was possible to get into them and change what was going on inside them. So it seems that it is possible. But again, it's a whole range of different technologies that are out there. That are used across the U.S. And different ones have different properties.

Harry Ridgewell: And are you able to talk about how secure the on-line voting system used in Estonia and in Switzerland in their referendums? Those systems, how secure they are?

Steve Schneider: They have a number of mechanisms to resist some of the possible attacks that can be there. They're introducing notions of verifiability whereby various checks can be made along the way. Not of the equipment and the software itself that's running. But on the output. So on the information that's being processed. In order for certain checks to be made to show that tampering hasn't occurred or changes haven't occurred. Or actually as well as security, that bugs haven't accidentally brought in some changes to what's goin on.

Harry Ridgewell: Sorry, is that Switzerland or Estonia that you're just talking about?

Steve Schneider: Well both actually. I think verifiability is an issue that generally is becoming more prominent in electronic voting. And I think both in Estonia they talk about aspects of verifiability and in Switzerland they talk about aspects of verifiability as well.

Steve Schneider: What you really want is what's called end-to-end to end verifiability where you can check every link in the chain from the voter creating their vote and submitting it in the first place. Right the way through the system of how its processed to the other end of where the votes come out and go on tallied. And that's what gives you the leap from individual votes going in to the final result coming out.

Steve Schneider: There are challenges in getting verifiability end-to-end. And I ... So for example, a voter might be able to check that the vote that they cast has been captures correctly. But then they may not necessarily be able to check how it's processed after it's been captured correctly. So at the moment there are certain layers of trust that there has to be in the authorities that are running the elections, they are managing those aspects properly.

Harry Ridgewell: And even if someone is unable to actually alter votes cast in an election using on-line voting of some kind, how easy would it be for someone to trace where those votes came from and identify the voters and basically publish how people in, certainly in elections or in the Swiss referendums voted?

Steve Schneider: Well again, I don't know how easy it would be for external parties to do that. But certainly the authorities that are running the elections would be able to trace back to individuals. What their, at least what their encrypted vote is. And they're also in a position to be able to decrypt it if they wish. So there is certain amount

of trust in the authorities that they're not doing that. But the system itself as I understand it, has that property.

Harry Ridgewell: Can remote e-voting or on-line voting be done securely without national identity cards?

Steve Schneider: I think it's very difficult to be confident when you're doing on-line voting of who the voter actually is. The national identity cards, the EID cards they use in Estonia provide a way of doing that. So you know that the person casting the vote is the person who is holding that ID card. It does seem to be very difficult to do without some equivalent mechanism that provides an assurance of who it really is at the terminal that's casting their vote. I think there can be ways of doing it by issuing credentials for individuals and relying on those credentials not being passed around or sold or not providing ways in which voters are not going to do that.

Steve Schneider: Then there are gonna be challenges around usability. So, if you've got some mechanism that you only use every five years, or some voting card that you only use every five years there'll be a large number of these that are misplaced and that where replacements need to be issued and that in itself can be a vulnerable area where new cards can be ordered up. So if you have something that's used very infrequently then it has to be very easy for voters to be able to pick up and use again. As it's, this is gonna be voters who are not necessarily security minded. They just wanna get on and vote as easily as possible. So I think it can be done but there are challenges around the usability aspect.

Harry Ridgewell: So an Electoral Commission 2002 report said that China, Russia and Pakistan are likely to have significant technical ability should they choose to attempt to disrupt the UK election. Has that changed and are there any other countries now that you think be added to that list if the UK was to adopt on-line voting?

Steve Schneider: Certainly I think there are a number of nation states that would have that capability and do have the capability to launch cyber attacks generally on ... And I think since 2002 I think that's a lot more. There's a lot more. I wouldn't want to name any particular countries, that's not my area of expertise. But certainly I would say there'd be a number of countries that have that capability if they would wish to use it to disrupt an election or to disrupt on-line activity generally.

Harry Ridgewell: Do you think it would be much larger than the three they already outlined? The use of ... And you don't have to say which countries, but five, 10, 20 ? How much are we talking?

Steve Schneider: Yes, I don't even know a number particularly. But I know there will be a number of countries that are developing, I guess, cyber attack capabilities on a nation state scale that enables them to conduct this kind of hostile activity. I don't know how many but I know it's going to be more common.

Harry Ridgewell: So the report also concluded, "It is logically possible for internet voting to be made suitably secure for use as the mainstream means of voting in a UK general

election." Do you advocate that the UK or any other countries take up on-line voting for their elections?

Steve Schneider: I wouldn't ... Even if it is logically possible to be made suitably secure ... Logically possible is an interesting phrase because we're also talking about suitable security is also having to take into account the human side of it and the usability aspect. If you have a system, which was kind of logically secure but was unusable, that wouldn't be so useful.

Steve Schneider: I think at the moment we're not at the stage where I feel that you could put your hand on your heart and say, "This is suitably secure against a well resourced attacker." And as the mainstream means of voting in a UK general election, I think there is still capability to disrupt.

Steve Schneider: There're different aspects. I've been talking earlier on about attacks where in the integrity of the election our votes could be changed and so on. But it's also with respect to disrupting an election happening in real time. You have denial of service attacks. And that's probably more likely to be the way in which an election could be disrupted. It wouldn't necessarily ... Well if you had targeted denial of service attacks that were launched in particular areas in order to swing the vote by preventing certain groups from voting then it could affect the result. But just in terms of disrupting it then casting doubt on the result, I think that's certainly within ... Well it's very difficult to defend against. You have to have mitigation. Ways of mitigating.

Steve Schneider: So I would say at the moment I think it's not yet ready for prime time. I would say with respect to internet voting. We see attacks all the time on other organisations that are fairly well resourced. I don't know how well resourced the political election authorities are in comparison to that. But it seems certainly possible that those systems could equally be vulnerable to the similar kind of attacks that we see in the news all the time.

Harry Ridgewell: Do you think that as technology improves that in the immediate future on-line voting could become secure enough to be a viable system? Or do you think that voting in person is always gonna be more secure than any kind of technological advancements bring to on-line voting.

Steve Schneider: Well, I think there are some aspects of voting in person that you really can't reproduce with voting over the internet. Being confident that the voter hasn't had somebody standing over their shoulder telling them how to vote for example is extremely difficult. And if you don't have control over where the individual is voting. And if somebody is voting from their own device they have to be confident that, that device itself hasn't been attacked. They have to also be confident that the vote that they're typing in is being transported correctly. So that's a vulnerability.

Steve Schneider: The Estonians do have some mitigation against some of that. So in particular they provide the ability to re-vote. So if you cast your vote electronically and you

have been leaned on, you have been coerced to vote in a particular way you can always go to ... On-line voting in Estonia is always before the election day itself. And on the election day itself they also have voting in person on paper. And you can always go vote on paper even if you've already cast an electronic vote. And then they will remove your electronic votes from the count.

Steve Schneider: So that's a mitigation against somebody leaning over you and telling you how to vote, is that you can ... First of all you can vote more than once any way electronically and they'll only take the most recent ones. You can vote again and correct it. You can even go on the day and cast your vote on some paper.

Steve Schneider: So there are ways of mitigating against being leaned on. The Estonians don't believe that, being leaned on is a significant threat possibly because they have this mechanism for guarding against that. But voting in person gives a more assurance that the individual really is being able to cast the vote in the privacy of the polling booth without having any undue influence.

Steve Schneider: Having said that, I think there does seem to be political pressure and social pressure to do more and more on line. And there is push for doing on line voting for the convenience aspect. And so I think it's important that we continue to do research in this area and see how and where the issues are and how they can be guarded against and to understand the risks that are being taken and the limitations with issues around it.

Harry Ridgewell: In layman's terms would you be able to describe how the Estonian voting on-line system works?

Steve Schneider: Okay, I guess I have to do it at a high level. But I haven't obviously voted in Estonia so I haven't experienced it first hand. But my understanding is that you use your electronic ID card and you plug that into the device that you're voting from so it does give an assurance that it really is you. That it's the person that has the ID card that is there at the device. And you'll be given the voting slip if you like on line. You'll be given the choices and you will make those choices and then you will submit those into the system. And you, I believe, that there is a mechanism for you to be able to check the vote that has been received really corresponds to the vote that you cast. You can have it read back to you via another channel. So that if you are concerned that if your device has been hacked you can see whether what's been received corresponds to what you thought you sent.

Steve Schneider: And then after that point the system has your votes and they are then processed securely by the election authorities and they, I believe they publish some verifiability information but I'm not really up to speed on the whole mechanism. Excuse me, there's just someone to the door.

Steve Schneider: Hello? No, I'm doing an interview but I'll come and find you when I'm done. Okay so we'll ... Yeah. Okay. So thanks.

Steve Schneider: Sorry about that.

Harry Ridgewell: It's all right.

Steve Schneider: Yeah, so in layman's terms what it looks like to the voter's point of view is that, they have a way of authenticating themselves and then they go into a website where they will select their choices and submit that into the system. Then they have a way of checking that what's been received by the system corresponds to what they sent.

Harry Ridgewell: Has Estonia experienced any State or notable cyber attacks since introducing on-line voting?

Steve Schneider: Well, yes I mean they did in 2007. This is fairly widely referenced. Not on voting system but they experienced cyber attacks on their infrastructure as a whole. So I think banks for example and broadcasters were hit on a denial of service attacks where they were just not able to provide the service that they needed to provide because they were being flooded both by traffic and ... In this so this was kind of orchestrated as much ... There was a whole range of websites that were attacked that prevented them from doing their business.

Steve Schneider: So that was in 2007. That looks like it would have been a demonstration of an ability to do that kind of disruption in a way, so ... It was certainly on a bigger scale and more sophisticated scale than standard denial of service attacks that had been seen before. The general consensus is that it was a State metal, if you like.

Harry Ridgewell: How secure would you say overall that Estonia's on-line voting system is?

Steve Schneider: Well they will certainly say that they haven't seen any attacks at least that they're ... They've argued that it has a number of security mechanisms in place that make it secure. And they have aspects of verifiability as I've said. Not just on the voter to be able to check their vote, but also as the vote's processed. But I don't know if they have the end-to-end verifiability. That's slightly different security. Security is about whether the system can be attacked. And what verifiability gives you is evidence that it has not been attacked. Or detecting on when it has been attacked.

Steve Schneider: I think it seems to be as secure an on-line voting system as you'll see anywhere in the world at the moment. So I think it's leading in terms of the on-line voting as I understand it. So I think it's leading in that. I would never want to say that the system is 100% secure, but I think they look at how to manage the risks. And a country of the size and the digital ability of Estonia they seem to be happy with that. The security level of that.

Harry Ridgewell: So you've written that on-line elections work well in low stakes elections. I was just wondering what kind of elections you think that, that includes?

Steve Schneider: So lower stakes elections I would say are elections that don't, that are not for who's governing. So these organisational elections. Or electing officers of societies or representatives. Those kind of things. So possibly trade unions'

elections. Possibly ballots on industrial actions. That's where the stakes starting to get higher. Because of what the results of the election will actually mean. So what I mean by low stakes is where there's gonna be less incentive for them to be attacked systematically by well resourced adversaries. So the stakes in a sense don't necessarily make it worth ... Bring it to the attention of such adversaries.

Harry Ridgewell: So I also read that the U.S. was considering using on-line voting for those covered by the Uniformed and Overseas Citizens Absentee Voting Act. I was just wondering if they did end up pursuing that? And if so, how secure that system is?

Steve Schneider: So I think different states do different things. And I think there are some that they, they do it in different ways. For example, some of them will do it by email. Where a voter or at least I've seen proposals for doing it by email. So a voter will get to complete their voting form into a PBF and possibly sign it in some way. Plus then they've gotta, their name is associated with it. And they'll email it in. Well that's horrendously insecure. Email is not a secure way of communicating anything.

Steve Schneider: With respect to on-line voting with overseas military they can vote electronically in controlled conditions. They can do it in a polling place and manage the authentication of the voter in a non-digital way. By using real ID and knowing who the voters are. Having authenticated themselves with documentation.

Steve Schneider: So they're having them cast their vote electronically into a system still needs the system at the other end where they cast their vote to be secure and I haven't seen comparisons as to how they will do anything more than standard procedures that where secure administrators try to take certain steps to provide security in their systems.

Steve Schneider: So I don't think it's at the security levels that ideally you would want. The balance there seems to be ... The argument is that while otherwise these people will be disenfranchised. They're overseas and they're out there living there on the front line for the country and you shouldn't disenfranchise them. And I absolutely agree with that. But that doesn't mean that risks should be taken with respect to them being able to cast their votes.

Harry Ridgewell: So also read that you worked on the Victorian Electoral Commission in Australia on a verifiable e-voting system, which was to be aimed to use in the 2014 Victorian State election?

Steve Schneider: Oh, that's right, yes.

Harry Ridgewell: I was just wondering if you could talk a bit about that and if that did end up being used in that 2014 election?

Steve Schneider: Yes, it was used in that election. So that came from the desire to provide accessibility to in particular blind voters, but partially sighted, motor impaired.

And then also to provide voting in languages other than English because they have to provide the ability to vote in 20 different languages. So that's where the demands came from. When they were looking at how to do this electronically they were concerned about the security aspect of their electronic voting so they, we got involved with providing a way of doing it verifiably. So introducing these ideas of verifiability so the way that the vote was captured ... It was captured and secured cryptographically and then the voter would get a receipt that corresponded to the vote that was submitted but in a way that didn't give away how the vote was submitted. But they could see that it hadn't been tampered with. But the receipt didn't show how they voted so they couldn't show it to anyone else. So they still had the privacy of the vote.

Steve Schneider: That was only for those particular voters that it was offered to and then it was also offered to voters in London that went up to Victoria House or Australia House in London, that could cast their vote remotely. There were about 900 votes that were taken there from Australians in London that went and cast their votes electronically. And they were all transmitted across to Melbourne. To Victoria Election Commission.

Steve Schneider: Then those votes were shuffled so that before ... In a verifiable way so that what the votes that come out correspond to the votes that go in and then they were decrypted so then they all of the individual votes were identified but in a way that they couldn't be linked to the voters. So that did provide end-to-end verifiability. Voters could verify that their vote had gone into the system in the way that they had cast it. Then the votes were processed in a way that's also verifiable.

Steve Schneider: Of course this was only for a subset of the voters. So the point where the votes were decrypted, they were then fed into ... Added to the other votes that had been captured on paper. From the rest of the voters. So they ran it for that particular demographic or groups of voters so it was in a controlled way. Which is what we wanted given that this was the first time this was being done and it was a new system that was developed.

Harry Ridgewell: So how secure would you say that, that system was in the end?

Steve Schneider: So the system was secure in the sense that it was verifiable and voters were able to check their votes and a number of them did check their votes. And there weren't any objections raised. So it was secure in a sense that the votes that came out we are confident, we can be confident that they correspond to the votes that had been cast.

Steve Schneider: At that point, that didn't give rise to an overall tally. What that gave rise to was a set of votes that were then included into the rest of the system. Then the electronic part of the system itself we have evidence that it was not attacked. So as well as using the standard security mechanisms that would have been used with respect to the private networking and so on, which is as secure as other systems that are like that. But we had this additional verifiability aspect that said

that actually, that the system hadn't been attacked. Or at least that any attack there had been an unsuccessful attack that had changed any of the votes.

Harry Ridgewell: Do you think that, that system was more secure than Estonia's?

Steve Schneider: I think for the aspects of the voting that it was handling, it's difficult to say without knowing the evidence of the Estonia. But what we did say is that it was the first time and end-to-end verifiable voting had been done. So I think that at that time we would have said, yes, Estonia's isn't end-to-end. It didn't have the level of verifiability that we demonstrated at that time.

Harry Ridgewell: Okay. Thank you Steven. That's all of my questions. Is there anything else that you want to add or talk about?

Steve Schneider: I don't think so. Not at this stage. I think the general question which I think that people want to know and that's very hard to answer is how secure is a system? Or is a system secure enough. And the work that I've been doing is almost ... It's on the assumption that systems will never be 100% secure. We're always seeing systems being attacked. And therefore something that, some additional mechanism that says even though this system is not 100% secure we can verify this particular run of the election has given us a correct result. So that's what verifiability gives you since it is essentially saying, well even if the system has been attacked ... And obviously we want it to be as secure as possible because we don't want it to be attacked because that's disruptive. But even if it has been we can detect and therefore we can limit the damage that can be done.

Steve Schneider: So, yes if there's a denial of service attack and the voting in Australia House could have been subject to a denial of service attack and could have been that the network had been overwhelmed and wouldn't have been able to get the connectivity we wanted. So you have a fallback mechanism there that voters could vote on paper anyway. So you need to have a way of managing when you've been attacked. But what you really don't want is for the wrong result to come out in an undetectable way.

Steve Schneider: So you don't want somebody to be able to go in and change the results of your election or influence the result of your election without you being able to detect it. And if you can detect it and you have evidence that this happened then that still bad news because you have to re-run the election, and that can be expensive. But it's better than having the wrong people winning because of some kind of attack.

Steve Schneider: So I would say verifiability is the key additional aspect that you want on top of trying to make these systems as secure as you can. Because you can recognise that no system is gonna be 100% secure.

Harry Ridgewell: And sorry, I don't know if we already touched on this but ... Do you fundamentally think then that voting in person is basically the best way to go about it?

Harry Ridgewell: With the exception of perhaps in remote areas or where people are disabled or blind or partially sighted with the exception of those groups, do you in general think it's safest just for people to go in person?

Steve Schneider: I certainly have a preference for voting in person. For voting under controlled conditions even if you're going to do that electronically. I think it is going to ... It is in general going to be safer than internet voting.

Steve Schneider: But I can see there is a push for internet voting and I think the risks need to be understood because I don't think they're widely understood what the risks of it is. And if they are understood then it's for politicians to make decisions around that. But at the moment I worry that the discussion is not at a sophisticated enough level to understand the risks. It's more around the level of well doing it on pencil and paper is very 19th century and we should move on. Not often looking at what is required in these systems? In a sense. And what are the risks to doing it.

Steve Schneider: So you have people that absolutely believe the electronic voting is the way to go and you have others that believe it should never ... That actually pencil and paper is fine because everyone understands it. And I do believe that there are ways of doing electronic voting in a way that, or at least that there will be. But I think there's more research that's needed and more work that's needed to bring that to a reality.

Harry Ridgewell: And besides Australia have you worked on any other on-line voting systems?

Steve Schneider: Not that have been out there. No, not that have been used in the real world. Although I have had, well the discussions. And I know the people that are behind the Swiss system quite well, so. I'm familiar with some aspects of that. But I haven't actually contributed to what the Swiss are doing with their on-line voting.

Harry Ridgewell: Okay. Thank you. Is there anything else that you want to add, or ...

Steve Schneider: No. That's fine for the moment. If I think of anything then I'll send it through.

Harry Ridgewell: Okay. And are you happy for me to quote our conversation?

Steve Schneider: Yes, I would say I am. Yes.