

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?

Matthew Rice: I think the first thing that we have to establish is that e-voting and remote voting are like ... There's a variety of different systems that are available, and they're mostly provided by private companies. So each of those companies and platforms will have different levels of security attached to them. They'll go through different processes. So it's quite difficult to make a singular statement about the security of online remote voting.

But to try and generalize, and try and get towards that, there have been concerns raised by security professionals both for kiosk electronic voting and remote voting. So using online systems. One in particular, the [inaudible 00:00:54] Street [inaudible 00:00:54] organization participated in 2014, and it was in the Estonian elections. Estonia have a strong commitment to digital-first processes, and are ... That peer-reviewed research showed that there were vulnerabilities in attack [inaudible 00:01:15] could be operated ... changing the counting on the server, but also changing the vote on a user's computer.

So that portion was all about where you placed trust in these solutions. That's really one of the critical areas. Where are you even placing the most amount of trust, and is that the secure place to put it? And comparing it to postal voting, there's obviously some concerns and calls in postal voting's security, but I think the most relevant point to make in terms of looking at those two, is that the scale of vulnerability in postal voting, where you would be intercepting whole trucks and running a scheme, an industrial web ... is possible to be done by an individual with a computer when it comes to online voting. So, the scale of vulnerability discovered in online voting is so much more profound than in postal voting, but, nothing is 100% secure. We can all establish that.

Harry Ridgewell: So how secure do you think Estonia's online voting system is? And do you think it's any more secure now than when it started? Because I've been told that they now have end-to-end verifiability. So does that give you more confidence?

Matthew Rice: So, we haven't done subsequent assessment in neither of the ... [inaudible 00:02:49] been able to catch up on anybody else's doing them. There has been undoubtedly improvements in technology since the original research was done, but I wouldn't be able to make a definitive statement about it. End-to-end verifiability is something that these systems should be reaching towards and reaching, go pretty close, and then in paper ballot voting, we're going to have to reach that same standard when it comes to online voting.

Harry Ridgewell: Okay, so for the elections 2014 and before, how secure would you say that those elections were, then?

Matthew Rice: Well, so the conclusion of that report was that the vulnerabilities were so profound that they recommended changing the whole system. [inaudible 00:03:50] Considering halting anymore online voting until those vulnerabilities were patched. So the security

researchers' conclusions were that those insecurities were so great that it had a very real effect on the potential democratic legitimacy of some of these votes.

The Estonian government did not accept those recommendations, but that recommendation should be a mark of how concerned the researchers were when it came to concluding about these vulnerabilities.

Harry Ridgewell: Do you think that no matter what technological advancements happen, voting in person by paper ballot is always gonna be more secure than voting either in person with some sort of online booth, or voting at home online?

Matthew Rice: No matter what technological development ... At this stage, we have to remain in the realms of the possible at the moment. At this stage, there is nothing more secure than pencil and paper. And that's not just an opinion of Open Rights Group, but actually U.S. State Department officials when speaking with to other countries when preparing their own elections, have remarked that, "You may not want to introduce remote voting until you're absolutely sure and you have a high confidence and trust in your institution and keep with the paper ballot because that is the most secure."

And voting in person and attending the polling place, is also more secure than postal voting in that regard.

Harry Ridgewell: And what do you make of Switzerland's online voting system, they've used in referendum, and is it more or less secure than Estonia's?

Matthew Rice: I haven't been able to look deeply into the Swiss system, and my understanding they do have some kind of [inaudible 00:06:13] technology that's attached to it but I couldn't say for sure because I simply haven't had any insight into it.

Harry Ridgewell: So I read that the open rights group, your experts analyzed e-voting systems in 2007 and 2008 in trial and live elections. What elections were these and what did you find it?

Matthew Rice: So these were the electronic voting trials that took place across the UK. Over ten years ago [inaudible 00:06:50] piloted electronic voting. They were predominantly [inaudible 00:07:01] kiosk voting, as I remember, although I'll have to double check that. And the Open Rights Group received technical server status at these pilots, and so we visited the online voting sites, actually, so there was remote voting there as well. So the technical observer status included that we need to kind of go in and assess the systems that were in place the physical structures and how the servers were held but we weren't able to examine or verify the servers and in any meaningful sense... and so that was a restriction that concerns those directors of the court... and that restriction and being able to truly audit and reverify the process was one that wasn't just for open righteous but also included the electoral commission and both candidates agents, so people who candidates nominate to oversee the count and also election observers.

There were problems in south box and swindle where votes were downloaded and counted and on computers that were controlled by supplier staff without any confident or agent and able to examine the process. So that's like the equivalent of someone

checking out a bucket of paper ballots in an empty room and counting them and then coming back telling the candidates and the agents, here this is the outcome of that. It's that that is a concerning thing, it's something that doesn't happen on any paper based system and it was part of the implication there wasn't sufficient verifiable indicators. The indicator's verifiability in the systems at that time and also we acted a member again that is private services and platforms that offer the systems that you don't, as a country you don't get to build a whole electronic voting system yourself so you're settling interfacing with proprietary technology and that where companies are not willing to give you full end to end access to assess all parts of their voting system.

That's a real concern from the 2007 pilot. Those concerns are also echoed by the electoral commission who said, that concluded no pilots, no further pilots revolved around voting should take place without changes in the planning process the quality assurance and the allocation for kind of preparation so like cancel staff and show the serv avant actually who will be running the election.

because they were so concerned about how opaque some of the systems became that it risked undermining the legitimacy of some of those votes.

Harry Ridgewell: Do you think that either voting or remote e voting system would be cheaper than a paper ballot system?

Matthew Rice: I think for the moment it would always that the adding to the existing costs. So, there'd be no, at this stage, there is no chance of [inaudible 00:10:38] replacing and either paper based or pen or postal voting and there simply too much reliance and on those methods to vote and we would never want to see the removal of the polling place from democrat prose. That's, there's that. There are principled aspects to it that a lot of people hold dear in taking that time. Not only with their dog to go and vote in person and so when you're looking at the costs bunch of people understand the proponent to this support of the voting talk about how it would just bridge the cost but often those models are based on replace it and existing methods and that simply never, not feasible for decades and at least so it's not it's not really a metric that's I think worth while exploring and at this stage.

Harry Ridgewell: Do you think remote voting can be done securely without using national security cards?

Matthew Rice: That a really interesting questions, I don't from what I see there isn't any voting system available that doesn't have, that isn't under pinned by a national identity card. So, Estonia has a really, really strong commitment to digital participation like you said they base the most of the digital process on their Estonian ID card and the stress edition as well. So, at this moment it seems like there isn't way to establish verification for online voting without having some kind of national ID card and of course that is one of the unique aspects to the UK's situation. We don't have a national ID card and another shouldn't necessarily create one just for the basis of performing online voting. But I think that's a really, that's a question that Governor Whales are going to be piloting electronic voting trials. There're going to have to think really hard about what they're going to deem as acceptable verification for people that want to participate in this and because

at the moment it seems like you're, either you need to have that national ID underpinning to really establish the security you do.

Harry Ridgewell: Does providing online voting boost voter turn out and does it tend to benefit any political parties or wings more than others?

Matthew Rice: So, on that first question, does it increase turn out? No, to put it bluntly while some opinion polls would ask for [inaudible 00:13:40] say they are more inclined to vote online and I think it just or it more looking at where online voting is being piloted and where its established and looking at the turn out there... because what a person says it will do and what it actually does are often very different things. So, if we look at somewhere like Estonia again, they've had electronic voting since and another decade so they're looking at a rich and they had their, there has been no significant improvement in turn out since the introduction of online voting.

By the number of people voting online has gone up, its not had an absolute number of turn out has not gone up. In the interest in pointing to all this is again people talk about how this will, online voting will engage the youth... actually the Estonian models shows that it was more likely to be the forty to fifty plus that would be using the online voting system and first time voters.

The same thing was seen in Norway as well. They had trials in 2 sets of elections and they eventually then decided that they were no longer going to, they weren't going to rule out electronic voting... and their conclusions again were that the youth, there was no significant impact on turn out and again it was more likely that it was older people that would embrace online voting and the younger people in fact felt a sense of obligation in model principle is taking the walk to the polling stations to vote. Maybe those things are unique to those particular countries but I think that we often talk about particularly in Scotland how similar we are to the Scandinavian models.

There, those studies and that research is probably much more decipherable than in polling like banding and sort of polling of people who didn't vote and whether they would if they could vote on their mobile phone and then because that's live actual turn out mapping.

So, on that second question, I don't, I haven't seen any analysis about the political affects of online voting and but there is an interesting question around how you secure whether there is a digital arms race involved in ruling out online voting so, for smaller parties that may not have as savvy digital it, if you have online voting what does that create for those well resourced larger parties that can commit resources to digital polling or digital campaigning and versus localized strong constituency based candidate say like independence within a certain constituency. So people have raised concerns about how this may exasperate some of the problems around smaller, smaller parties being able to remain in solid in an election front but that's merely suggested I haven't seen any kind of suggesting there's any real effect, politically on online voting.

Harry Ridgewell: So in the US, some states you can vote by email or web portal. How secure do you think that is?

Matthew Rice: I mean there as secure, they'll be as secure as a fishing attack. Rights? Its the same, I thin one of the things you have to remember is that a lot of these systems are still based on still based on computer systems we would all use for other processes. So, there isn't a kind of a whole, although there's an e sector who will build systems that will allow you online votes to be cast. They don't build their own physical infrastructure. They still rely on the same servers that Microsoft relies on. So, it means they come into the same environment of risk and vulnerability as anybody else. There is also a level of social engineering that is attached to that as well. So, we can all have, we're all vulnerable to a fishing attacks and emails that report to be from a person that you believe that they are from who they say they are and you give out, you inadvertently give out your information. So, often people talk about how they like to think about these things as two very separate kind of environments but there not, they participate and exist in the same vulnerable schizophrenic digital environment that all of our other systems work in.

When we think of online voting we should think about it just in the same way. That we can go at any other large data breaches or cyber security risks that we've seen and growing and that recent years.

Harry Ridgewell: Is it much easier to trace who and how they voted if you vote by email rather than using say Estonia's online voting system because at least in Estonia you've got the National identity card. Whereas if you vote by email they've got your email address and probably your name in it. They can, is it much easier to trace if someone vote by email?

Matthew Rice: That's a good question, I don't know but I mean I think the most important aspect lies that the security of the ballot is the greatest protection against voter [inaudible 00:19:49] alternate issue. But I don't know whether or not voter identification is easier as result of emailing, email based voting, if there was any level of being able to identify the person, if the person was that voted. The [inaudible 00:20:07] that's simply is confidently in my one of the strongest against, one of the strongest protections for creating our goal. Which is that no one should know how you voted. There should be no way in which a person can find out how you voted... it is otherwise returned to the same space that brought us the secret ballot which works, bosses intimidating workers to vote particular ways, or business partners influencing families and whole communities votes, being intimidated to vote a particular way. That's where if you like for that kind of system to come back in for some kind of false sense increased [inaudible 00:20:57] not only do you risk not improving turn out you risk undermining peoples trust in the system.

So when, to defend, get defend core points across your [inaudible 00:21:09] any election system has to satisfy these 3 conditions. It has to be secure, your goal has to be secure the steps plus you're taking that it can't be tampered with. It also needs to be anonymous. So, your vote can't be traced back to you. Which protects you against coercion. It also does need to be identifiable. So, it has to be saying that one person cast this one vote and didn't cast another. To be kept and but then by being identifiable it also needs to be secure and anonymous, and that's the core problem. That's the biggest kind of issue with electronic voting. It struggles to satisfy all of these conditions at the same time. Whereas with paper ballots its tense but the bounds between those fundamental conditions are satisfied.

Harry Ridgewell: Do you think that any countries are likely to adopt or drop online voting soon?

Matthew Rice: I don't know of any countries, we are proceeding that Scotland and Wales are piloting online voting and it's all about how they structure that. None of those pilots should get local or governmental elections because recently they haven't shown, since the 2007 trials the e voting can work in the UK's specific environment with all the security things being discussed around national identity cards and things like that. It is interesting to see how France recently dropped online voting with concerns about cyber security. I think the Finns also, Finland recently dropped it, although we need to double check that of course go in this transcript. There are, it does seem that at this stage there are more countries that are halting online voting and then there are racing into it. There are obviously some states in America that are doing these different trials and often working on state based elections but I think voter confidence is one of these things that are at the lowest end and people are still deeply concerned that voter identity and interference can take place in these systems and so they are being very weary about introducing it.

I think, just thinking about it, if 1 country is adopting it does not mean, does not make it does not give it a green light for others. Every country has a unique set of problems and issues and social constructs that need to be considered. So say, just because the French dropped it, the Norwegians dropped it, doesn't mean that the Swiss have to drop it as well but in Europe I think it's fair to consider whether or not there's similarities or differences in those countries that have to meet and are like compared and thought about in our context in the UK for going ahead.

Harry Ridgewell: And finally does the open rights group advocate that the UK take up online voting for general elections?

Matthew Rice: No, we don't advocate that like I said, many UK electoral environment is very different to all the other countries that we have discussed and so there are some unique challenges that online voting may not be able to satisfy because of some of the systems that we have or don't have in place. So, at this stage it would be very concerning to see them in the upcoming general election any kind of online voting would be ruled out. One of the most important aspects of all this is, this is critical infrastructure and it should be assessed based on those kinds of principles so you know the National Cyber Security Center, NTHQ, should be heavily involved in assessing the electoral environment and how these systems operate to make sure we are, the integrity in the democratic process in the UK is maintained and we can not reach, it would be foolish to reach for greater participation at the risk of losing ultra confidence and trust because it would not only potential not move participation or turn out anyway and you would not improve participation and turn out you might actually reduce trust, confidence and then, that can in effect reduce turn out for further elections.

That's gonna create risk with a badly implemented and poorly constructed online voting system and at this stage, we can take, and we don't have that system, it's not clear what system is there that will satisfy the conditions that we've created.

Harry Ridgewell: An electoral commission 2002 report concluded it is logically possible for internet voting to be made suitably secure for use as the mainstream means for voting in the UK general election. What do you make of that statement?

Matthew Rice: It's logically possible it comes, its one of these [inaudible 00:27:11] between like an academic that says there's a mathematical proof that such a thing can take place and an [inaudible 00:27:18] saying well we can't find the actual environment to establish it.

I think one of the things we didn't discuss I guess is how we, how people, what people do to, why people trust elections problems. So one of the things is that can't, can an losing candidate accepts that they lost the vote. That's the most important part of any voting system, or any vote. It's not the winning and the voting, it's the candidate and the losing. Saying something is logically possible to rule out, upon a mathematical trip, there's not include consideration of the disgruntled loser, who stands up and says I think this has been fixed. I don't understand this system, they're talking about block chain and cryptography for instance and I think the fix is in. They do that, their supporters rally all of a sudden you have people asking questions.

It doesn't really matter that something's logically possible, it's whether something is politically vulnerable, as well and you should not be introducing something that doesn't have the, trust and confidence across the system that will result in a candidate who loses and ... accepting that result. So, that's one of the one really cool parts and it could, why the electoral commission said that in 2002 about the kind of logical possibility of it, actually most trials run in 2007 and we saw practical reality of what it was like to try and operate an online voting method in the UK. Their conclusion was no more trials until we satisfied a whole bunch of other conditions. I think it's more important to look at what 2007 showed which is the limitations or practically of this than discussing this on a kind of theo-ethical and academic stand point.

Harry Ridgewell: Do you think that block chain online voting isn't secure either?

Matthew Rice: I wouldn't know, I don't have huge amount of insight into block chain and got a do thing that are [inaudible 00:29:36] kind of emphasize that it's not just about the mathematical proof. It's about people feeling like they can trust a system and that as you've seen feelingless and are can be much more effective than facts and in this scenario we have to just be aware of that when we introduce it. Ultimate I don't think it's, I think there's probably opportunities out there for blocking technology to improve it in some ways but it still needs to be looked at form the lens of what is, what does this mean for the public, how does the public understand the process at the end of the day.

There requires them to understand block chain technology, is that really going to be the, is that rally doing to be a realistic, a realistic task. A realistic standard for you to expect the public to reach.

Harry Ridgewell: OK, thank you. That's all of my questions. Is there anything else you want to mention?

Matthew Rice: No, I don't think so. Like I said we've got these trials that are being talked about in Scotland and Whales. So [inaudible 00:30:57] are really interested to hear from anybody

who's interested to kind of participate potentially in [inaudible 00:31:05] or kind of watch them be these potential pilots. So, if anyone is interested we are currently in the process of considering our options and I would be delighted to kind of sit down and discuss with others about how, what kind of involvement people would want to see in this. Ultimately, it's a public process and so we should have as much of the public involved in these and so I hope then people reading these articles that will read your article and if your interested take time to kind of engage in taking a bit more, longer look at what these pilots and what they look like. We will find out more in the summer in Scotland. I'm not sure what the timing is in Whales.

Harry Ridgewell:           OK, Thank you.