Harry Ridgewell: How secure are e-voting and remote e-voting? Are they any less secure than voting in person, or by post?

Peter Ryan: Hold on. You want to contrast ...

Harry Ridgewell: How secure e-voting and remote e-voting are. Are they any less secure than voting in person or by post?

Peter Ryan: Basically this is the difference between remote voting and in-person voting, right?

Harry Ridgewell: Yeah.

Peter Ryan: For me, “e-voting” is a broad term, which can cover both potentially. The first answer to that is that, broadly speaking, obviously remote voting is much harder to make secure than in-person voting station voting for the obvious reasons. Because in person, you can at least have some guarantees of the isolation of the person at the time that they cast their vote, in the booth or whatever, it is very hard to try and simulate that in a remote context, whether you're doing postal, or internet, or whatever. Broadly speaking, it's much harder to make remote voting secure.

To put it differently, I would say that I think now we have some schemes which have in fact been implemented and deployed, or at least trialed, which provide very high levels of security for in-person voting, voting station voting, but I don't believe that at the moment we have any technology, any scheme which can provide a sufficiently high level of security, at least for parliamentary elections and so forth. It is my view that no scheme which currently exists can provide that level of security for remote, particularly internet voting.

Harry Ridgewell: Do you think that no matter what technical advancements appear in the near future, paper ballot voting is always going to be more secure than voting online?

Peter Ryan: I'm not sure I'd go as far as that. Who knows what technical advances we'll come up with? I come from the computer security, information security, crypto community. We have been making significant strides over the last few decades in improving the security of both in-person and remote voting. There may well be some advances in the future which would allow us to do online voting securely.

Paper, fundamentally, always has a lot of fairly special qualities, which are good from a voting point of view. In fact, in collaboration with Steve Schneider, I've worked on a scheme called Prêt à Voter, which Steve's probably told you about, which is an in-person, voter-verifiable scheme. The voter actually there does walk away with effectively a paper receipt which has an encryption of their vote. They can later use that as evidence to show whether or not their vote has been accurately recorded on a web bulletin board, or public ledger, whatever you

want to call it. That's an example of where we have a combination of paper and electronic cryptographic techniques. I personally think that at the moment, that's the way to go with these schemes, to have to have the qualities of both the cryptographic and paper.

Now, if you're doing online voting, of course it's not really quite clear what role paper can really have. Maybe the voter can print off something at home, and maybe that can be digitally signed, and so on, but the role of paper, it seems, strikes me as less clear there.

Harry Ridgewell: Can remote online voting be done securely without national identity cards?

Peter Ryan: One of the key problems, besides all the other insecurities of the internet, one of the major challenges obviously with internet voting is how do you authenticate the voters. Without something like an ID card, it's very hard for me to see how you really do that, particularly if you want to have what we call a universal eligibility verification. That's a requirement that anybody should be able to check that votes that have been cast and put into the tally have all been cast by legitimate voters, and each voter has cast at most one vote. If you've got something like an ID card, like the Estonian one that can apply individual digital signatures from the voters, then you have a means to do that.

If you don't have something like that, I don't see any way that you can really achieve this property of universal eligibility verifiability. You can do things like send out credentials by email or something to voters, which some voting schemes do, but that's not really going to be very secure. Even if there's some other way that you can get voters to apply their personal digital signatures to, say, an encrypted vote other than having a national ID card, then maybe you can.

Harry Ridgewell: Would either online voting at a polling station or remote online voting be more or less expensive than a paper ballot system?

Peter Ryan: That's again going a bit beyond my area of expertise into the economics of this thing, but it's certainly true that running conventional elections is typically pretty expensive, paper-based. I guess in principle, online voting could be less expensive than conventional paper voting, but you've got the initial expense. First of all, we have to get to the stage where we've actually developed, and certified, and so on, a secure online voting system. The cost of that is going to be nontrivial. Once you've got over that, then I would imagine that costs should be lower. Whether that's an argument for going that way, of course, which is maybe the implication of your question, is something which we have to debate as a society.

Harry Ridgewell: Blockchain online voting is only something that I have recently read about. I was just wondering how long that's been going for, and if you could describe how it works and how secure it is.

Peter Ryan: It's a fairly new phenomenon, just as blockchain, public ledgers, and so on are fairly new. Certainly, we keep hearing about new suggestions to do blockchain voting, or voting with bitcoin. I've heard suggestions. I personally am actually quite dubious about many of the claims. You hear claims that blockchain can solve the online voting problem. In my view, that is completely false. Blockchains can potentially help with one aspect of the system. For decades, people like myself have been working on secure, cryptographically-based voting systems, both for remote and in-person.

Typically, those schemes have always used some notion of what we tend to call a public bulletin board, but nowadays as a trend of blockchain, you might call that either a blockchain, or a public ledger, or something. This is basically an append-only board which is an unsecured broadcast, so you guarantee that anything that's posted there stays there, and that everybody has a consistent view of the contents of the board. This is a crucial part of many of the schemes. Clearly, that's a public ledger of some kind. It's possible blockchain-type technologies might ... could help with implementing that component in a secure voting system, although even then, it's not clear to me that the kind of decentralized, permission-less kind of blockchain that, for example, bitcoin deploys is actually the right thing to be using in this context.

All the other problems, which are the really interesting problems of voting, like how do you authenticate voters, how do you guarantee their anonymity, how do you counter threats of vote-buying and coercion, all those problems, blockchain really doesn't intrinsically do anything to help. I've taken a quick look at a few of these schemes that have been proposed. Frankly, none of them have impressed me very much. I don't think they actually buy you anything beyond the kinds of schemes that already have been proposed. I developed a system called Pretty Good Democracy a while back, and as a team more recently, I've been working on one called Selene, which is designed to provide a much more direct, intuitive way for voters to verify their votes in the tally. All of these schemes provide very high levels of voter authentication, coercion resistance, and so on. I don't see how a blockchain scheme gets any particular advantage over those kind of schemes.

Harry Ridgewell: In the U.S., in some states, voters can vote by either email, fax, or web portal. How secure are any of these methods?

Peter Ryan: Clearly, none of them are really particularly secure. Email is notoriously insecure. Fax, possibly, is marginally more secure, but even if you trust the channel, you're still having to trust whoever's at the other end, who receives the email or the fax, to handle it correctly, not alter it, not violate the privacy of the voter who cast it. I would say those kind of schemes intrinsically are highly insecure.

Maybe this is a point to jump back again. The kind of stuff that, again, I and others have been working on is to try and provide schemes which require

minimal trust in the software, the infrastructure, the authorities, and so on and so forth. The guarantees of privacy, accuracy, and so forth all arise from cryptography and mathematics. You put the ability to check that things have gone correctly back in the hands of the voters, in some sense. These kind of schemes where you send in a fax or an email, basically, you implicitly have to trust whoever's at the other end and is going to handle your fax or email, both for the integrity of the vote and for the privacy of the vote. I would say that they're hopelessly insecure.

Harry Ridgewell: Would it be very easy for them to identify who you are if you voted by fax, or email, or web portal?

Peter Ryan: Typically, yes. It depends, I suppose, what safeguards have been put in at the other end. Obviously, if it's just some guy at a server who's receiving emails from someone, the sender of the email is typically very easily identified. Unless you're going to start using Tor and stuff, which I think most voters are typically not going to be using.

Harry Ridgewell: How secure would you say Estonia's online voting system is?

Peter Ryan: Well, it's better than email or fax. They certainly have tried to put in some measures to achieve a level of security. I haven't looked too deeply at all at the details. Particularly, I think they've introduced some innovations recently which improve the situation a bit, but their standards are the kind of schemes that Steve, and I, and others have been developing. Their security is not that great because it's not what we would call universally verifiable, which basically means that any observer can look at the evidence that has been produced as the election unfolded and concur that every vote has been properly processed and so forth. In the Estonian system, you still need a very high degree of trust in the authorities that are running the election.

The other important point is that as far as I can see, there is nothing really very much in the Estonian system to counter vote-buying and coercion. If you've got a coercer who is shoulder-surfing while the vote is being cast, I think the only counter in that case that they have is for the voter then to go and I believe they can recast, potentially in person, and that overrides the electronic vote. That is a not unreasonable measure to counter coercion, although it's obviously not terribly convenient for the voter, who will have to go then and vote in person to override the coerced vote.

I would say that the Estonian system is, amongst the systems which are deployed, is not bad, but it could certainly be hacked by a determined adversary, like a nation-state adversary. I'm quite sure it could be hacked. How worried they are about that in Estonia is not clear to me, but it should be, I think.

Harry Ridgewell: What about Switzerland's online voting system that they've used in referendum? How secure do you think that is, and how do you think it compares?

Peter Ryan: Good question. Again, I haven't looked. They have a number of systems, I think, in Switzerland, and they've been evolving. I haven't looked in depth at the details of this latest system which they are proposing. I recall the latest system has a sort of confirmation code mechanism, so the voter gets back some kind of code which they can check on a paper sheet that they get. That gives an indication that their vote has been correctly recorded, although again, that's not something that they can really verify in a meaningful sense. They still have to trust the system that records their vote and sends the confirmation code back.

It's a moderately secure system. I would say again, against a determined hacker, particularly perhaps an insider attacker, you could certainly manipulate the vote, but it's a reasonably good system. I think they're going in the right direction. They are seeking to try and improve the security of it. In terms of coercion resistance, I'm not quite sure how they handle that. I suspect, if I recall, they also have a re-voting scheme so you can re-vote later when hopefully you're not being observed, and override your earlier vote. But again, I would have to check the details of that.

Harry Ridgewell: Do you think that countries developing or which have online voting systems, their systems should be completely internal and they shouldn't outsource anything to private companies? If they were to outsource to private companies, does that make it inherently less secure?

Peter Ryan: Well, it depends a little bit how you do the outsourcing. If you're using open source, you're just getting a company to develop the code according to your design. The code can be examined by experts. Outsourcing in itself isn't necessarily a bad thing. I think I would say the real difficulty is, for example in the U.S., they've had lots of voting system technologies that as you know were developed by private companies, and the code there is typically proprietary. Experts in most cases cannot get access to the code. Where they have managed to get access, sometimes because it was inadvertently leaked online, it was found to be hopelessly insecure. In that kind of circumstance, clearly the security you'll get as a result will be pretty hopeless. You certainly can't guarantee any kind of level security unless you can examine the design and the code. As long as that's true, I'm not sure it matters too much who developed it. It wouldn't have to be developed internally by a government.

Harry Ridgewell: Even if someone can't actually influence how the votes are taking place, in an online voting system, how easy would it be for someone to trace the voter's identity and find out how people voted?

Peter Ryan: Sorry. I didn't catch the beginning of that question.

Harry Ridgewell: Even if somebody can't influence votes in an online voting system, how easy is it for them to trace voters' identity and find out how people voted?

Peter Ryan: When you say can't influence votes, I think what you mean is, “can't influence the vote once it's been cast?”

Harry Ridgewell: Yeah.

Peter Ryan: Once it's in the system, so you're not talking about influence in the sense of coercion or influence at the time that the vote is cast. I assume that's what you mean.

Harry Ridgewell: Yeah. I'm just talking about people afterwards, for example, publishing, "Here's how everybody voted," and tracing how people voted.

Peter Ryan: I think the answer to that question will depend very much about the system we're talking about. The kind of systems, again, that I and others have been trying to design using cryptographic techniques try to provide very high guarantees that ballot secrecy will be guaranteed. Typically, with quite a lot of those systems, that does depend on what we typically do is use threshold crypto to spread the trust. There will be a set of trustees who hold shares of the decryption keys. As long as you don't get a threshold set of these trustees colluding to compromise the privacy, you should be fine. As long as you choose from a set of trustees that are perhaps mutually distrustful, from different parties and so on, that should be okay.

Most of the other existing systems we talked about, I suspect particularly an insider can probably quite easily break the privacy of individual votes. Another long-term issue, of course, is if you're using cryptographic techniques, you have to worry about the long-term secrecy of algorithms like RSA and “El Gamal” [inaudible 00:21:26] and so forth. People are starting to become seriously concerned about that in the longer term if we get quantum computers. We know that there are quantum algorithms which would break the major public key algorithms. That's something we would have to worry about even with a well-designed cryptographic system, but again, researchers are looking into these issues, and looking at post-quantum secure, or even in some cases unconditionally, everlastingly private schemes, which don't depend on the computational power of the adversary.

Harry Ridgewell: The voting systems which you've worked on, have they been used in any political elections?

Peter Ryan: Yes. I think I mentioned Pret a Voter earlier. Steve may well have raised this when you interviewed him. We did actually work on an adaptation of that scheme for use in Victoria state back in 2014. If I recall correctly, it was a lower house election. That was used for real, albeit on a fairly small scale. There are some other schemes which have been used. A scheme called Scantegrity, which

was developed by David Chaum and others, that was used I think twice in Tacoma Park in the U.S., a county in the U.S. There has been a little bit of usage, trialing in real elections these kind of schemes, but so far very modest. We obviously hope to change that situation and start having them more widely deployed, at least for in-person voting.

Again, for internet voting or serious binding political elections, I for one would be very nervous about pushing them, but I think for lower state elections, like companies and so forth, professional bodies and so forth electing officials there, then probably internet voting provides a good scheme. The current scheme probably provides adequate levels of security, but I would stress, for electing the president of the U.S. or something, we don't have any technology which is secure enough at the current time.

Harry Ridgewell: The Victorian state election online voting system that you worked on, how secure would you say that that system was?

Peter Ryan: That system was pretty good. Pret a Voter, I would claim, has very strong guarantees, both of verifiability of the integrity of the vote and the privacy of the vote. Unfortunately, when we were doing the adaptation for use in Victoria state, we had to make certain compromises which were demanded by the Victoria Electoral Commission. Some of the guarantees, the strengths of Pret a Voter, were watered down in that version. It was called vVote, by the way. It was somewhat watered down, at least for that trial. Although I would claim Pret a Voter gives a very high level of security, I would make more guarded claims about the vVote system that we used on that occasion. I think the security was probably adequate for the scale on which it was used. If it were used again, we would hope that we could develop a much stronger version to try and avoid the kind of compromises that we were forced into at the time, partly because of time scales to deployment and so forth.

Harry Ridgewell: Have most of the voting systems you've worked on, then, been used in companies to elect people within the company, like you were saying a minute ago? Is that predominantly what most of the work that you've done has been used for?

Peter Ryan: The schemes I've been working on have predominantly been in-person voting. I guess that's not particularly suitable for companies and so on and so forth, where I guess they want internet voting. The Pretty Good Democracy scheme, which was internet voting, that exists on paper. We didn't ever develop that into an actual scheme. The newer scheme that I've been working on for I guess about 18 months is the Selene scheme.

We are actually developing prototypes which we will be trialing now, and hopefully ... In fact, there is a project in conjunction with Steve, which again he may have mentioned to you, the Volt project. We're working with the electoral reform services companies that do online voting for companies and so forth, or trade unions, etc. We are currently working on developing a prototype for

trialing with them for companies. I would hope that in the not too distant future, within perhaps before the end of the year, we might actually have some trials run.

Other than that, most of my work has been fairly academic, shall we say, theoretical. There are some schemes like the Helios scheme you may have heard about. I don't know if you've talked to other people. Ben Adida some years back developed a scheme called Helios for internet voting, which is actually a pretty good scheme in many ways. It does provide voter verifiability. Ben is very clear though that he doesn't provide anything, really, in terms of coercion resistance. Again, it's not a scheme to be used for binding political elections, but that has certainly been used for, for example, electing presidents of student unions. It was used to elect, I guess, the rector of the University of Louvain, Belgium. That has been fairly widely used, so there are cryptographic schemes which have been used, but not in diplomatic elections, apart from the Estonian system.

Harry Ridgewell: Which countries would you say have the capability to conduct large-scale cyber attacks capable of influencing online voting systems used in political elections like in Estonia and Switzerland?

Peter Ryan: I suspect most decent-sized, advanced countries could do that. The obvious ones that spring to mind as probably the most advanced in this area, Russia clearly, highly developed hacking skills. In America, the NSA clearly also have. China has. The UK has pretty sophisticated cyber warfare capabilities. I'm sure the Israelis have, as well. There's plenty of countries that I'm sure would have quite easily the power to hack any of the existing internet voting schemes, if they put their minds to it.

Harry Ridgewell: Is there any evidence that any countries have either successfully or unsuccessfully tried to conduct cyber attacks on a country's online voting systems?

Peter Ryan: Evidence here is typically rather hard to come by, but if we look to the U.S., it does seem clear that there were attempts to mess with at least the electoral system. The U.S. fortunately, up until now, hasn't had any major deployment of internet voting, online voting, but they do, for example, keep electoral records on servers and so on. There does seem to be pretty strong evidence that some of those servers were hacked. Whether much manipulation was done to those records is not really very clear, I think, at the moment. It may have been principally privacy rather than integrity that was violated.

Harry Ridgewell: Which election was that, sorry, that you said that there was evidence?

Peter Ryan: This is the 2016 presidential election.

Harry Ridgewell: Right, okay.

Peter Ryan: It's pretty clear that quite a lot of things happened, there's certainly potential for some of the machines but although does know where to use, as I said, online voting very much, and there are certainly plenty of voting with machines, touch screens and so on. I think it's particularly true, in Pennsylvania for example. Some of these machines don't have paper backup records. So there would certainly would have been potential to manipulate votes cast on such machines. But part of the problem is that if there was manipulation, it could be done in a way which would leave virtually no trace. So almost by construction there probably wouldn't be evidence even if there had been hacking.

I think the answer is, maybe there are people in the FBI and so on who know more and have access to more evidence than is available in the open, but i don't know. I'm not currently aware of any clear evidence, that for example votes were actually manipulated in the 2016 election, but it's certainly clear, technically, that it could have happened, and it could have happened in a way which would not lay down any evidence.

Harry Ridgewell: Finally, do you advocate that countries adopt online voting for political elections?

Peter Ryan: Okay, if it wasn't clear from what I said earlier, in the current state of play I certainly would advocate that. I'm all in favor of doing research into improve the security of online voting, developing new schemes and then test them, but my firm view at the moment is that we have no technology or scheme which can provide adequate levels of security. So I would not advocate it at this point in time, no.

On the other hand, for lower stake elections some of the better schemes are probably okay. Like I said, companies, student bodies, professional bodies, and so forth. There schemes which are probably okay for that, for example. And hopefully very soon Selene.

Harry Ridgewell: I actually have thoughts, one other question. Which countries would you say have the best online voting systems in the world, and which ones would you say have the worst online voting systems? I'm talking about for political purposes.

Peter Ryan: I think there are very few countries that have actually deployed it, apart from Estonia and Switzerland.

Harry Ridgewell: Haven't ... I don't know whether it's just trials at the moment, but haven't Canada used it a bit. Alaska maybe, I don't know if they've stopped doing it but I think they did do it for a bit. I don't know if they're still doing it. I know France did it.

Peter Ryan: They might run some trials. I know France for a while was running internet voting for ex-pats[inaudible 00:34:01], but they actually stopped that in the wake of the 2016 US election precisely for these kinds of concerns about the

security. There have been small scale trials in lots of countries, but in most cases they've not been continued. So I think the only countries I'm aware of where online voting is used routinely for political elections is Estonia and Switzerland, I think. I guess we've already talked about the comparative security of those. Both are reasonable.

One of the points about Switzerland is these can't limit the percentage of people that can vote online for political elections. The limit depends, I think, on the level of security provided. So it actually seems to me quite a sensible move. If I recall correctly, for example, if you want to allow up to 10% of the electorate vote online you need to provide some sort of voter verification. So that means to me as a sensible move.

Estonia, I think, are taking higher risks in allowing essentially everyone, in principle, to vote online.

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

Peter Ryan: I think I've said I want to say.