**Eric:** So on today's Encrypted Economy, we have Alistair Muir from Australia, the CEO of Vanteum, and they do a lot of advisory services on privacy-enhancing tech and all that stuff. Now I got introduced to these guys through the Privacy Enhancing Technology Summit and Boston. I'll drop a link in the show notes.

I'm gonna be doing an armchair fireside discussion at the end of the conference, I think. So at any rate, they introduced me to Alistair Muir. He is a leader, thought leader in terms of privacy-enhancing technologies. And so I think it's really exciting to see how thought leaders are approaching this outside of the US and Europe, where we do a lot of our show focuses.

This is really a window into worldwide adoption, and this is not a technical discussion by any stretch. It's really just intended to provide a different lens for understanding Worldwide adoption. So what does adoption look like? What is the challenges experience? Where is the opportunity?

How are governments responding to it? And I invite you to listen, to find out. So if you enjoy this, share it with others.

Welcome to The Encrypted Economy, a weekly podcast featuring discussions, exploring the business laws, regulations, security, and technologies relating to digital assets and data. I am Eric Hess, founder of Hess Legal Counsel. I've spent decades representing regulated exchanges, broker-dealers, investment advisors, and all matter of FinTech companies for all things touching electronic trading with a focus on new and developing technologies.

The Encrypted Economy is excited to have Alistair Muir CEO of Vanteum on the podcast today.

Vanteum is an advisory business for open banking and financial services located in the down under. So Alistair welcome.

**Alistair:** Thank you very much, Eric. Thanks for having me.

**Eric:** We're gonna be talking a bit about privacy-enhancing technology today and adoption in Australia and other parts of the world.

But before we begin with all of that why don't you give us a little bit about your background and how you found yourself you know, Vanteum, and entering into the space of privacy-enhancing technologies.

**Alistair:** Yeah. Fantastic. Eric, thank you. So I suppose my background is a strange old blend of digital product venture, that data commercialization side, but also FinTech as well. So I've been a founder of a FinTech but also worked with a number of fintech here in

Australia. As well as helping some international fintechs make their market entries into this region as well.

But I suppose I've been working in data sharing and open banking for quite some time. And in fact, actually been working in open banking before it was regulated in Australia and New Zealand. And so I've been advising some fortune 500 financial services including banks, large general insurers and that sort of thing on both.

Data sharing and data partnerships, but then also the open banking and how can a large bank, for example, put a proposition to a customer that, that, that helps them grow their customer base, help them acquire new customers, but also adds value to the existing customer base as well.

So I suppose the other thing, just in my background to tease a, is that I've also worked a lot with our national science agency here. So the CSIRO here in Australia and really helped their Sytech accelerator to, to, with the commercialization of science and technology.

So really that's about helping researchers and scientists have, you line of sight to industry and solving industry problem with their research and then helping them learn the commercialization skills to then be able to, once they've identified that of line of sight, actually being able to accelerate things and actually turn, turn the technology into businesses and get the capital they need. So as part of that, I suppose I've worn several hats. One, one has been as a, a pro bono mentor to some of the founders in the accelerator. Also an advisor to the program to help it get scale. But then also I've been an entrepreneur in residence within that pro within that program, going deep with a couple of different ventures to accelerate that commercialization.

So I am proud of the work that I've done there simply because we've through that work spun out, I think 63, 64 new companies from world-class science technology. And I think it's one of those things. And you'll hear it come through, later on, but it's one of those things that I'm really passionate about, which is if you can get that line of sight to an industry problems and commercialized science technology, you can have a real impact.

You can have a real impact with that. You know, with getting research outta the lab and in, into the market I.

**Eric:** Excellent. Um, and in terms of that moment where you first realized the importance of privacy-enhancing technologies, and I know you and I had spoken about a particular project that you're working on, where you suddenly started to realize all the different issues use that arose with privacy.

Do you wanna expand a bit on that?

**Alistair:** Yeah, sure. Thanks, Eric. I think so, so naturally as part of working in any. Heavily regulated industry and trying to put data partnerships together between, say an insurer or a bank or an insurer, and even a telco that there are you know, I, I had, lived the challenges of trying to get those data partnerships off the ground.

And, and actually with broader than any single project, but the sort of challenges. Challenges we encountered regularly were actually, you're in a heavily regulated environment. It's what can you do with that data? Who can you share it with and what, for what purposes, that, that was a constant issue? And then you've got. The natural legalities around, around you know, what you can and can't do with data anyway. So certainly privacy is one aspect of that privacy in terms of the legal part, but also privacy in terms of you wanna make sure that you're doing the right thing with the data that you're the custodian of.

The O the other part, I suppose it was. That became very evident to me. Was that in, in a lot of these partnerships, regardless of what sort of side you were on, there's a lot of commercial sensitivity in inside of the, the actual data itself. So what if the other party learns something from the data that we have that reveals something commercially sensitive about our business?

You know, and then another big part of the, this is trust. So how much do we trust the other party that we're actually sharing this data with? And then to overcome. Some of those challenges or at least to address some of those challenges, different organizations have, different data governance requirements.

And before it, you start then going what do we then need to do to this data to minimize some of these risks? And so you do stuff to the data. Mask certain fields, you remove, fields with AI in them. You use aggregation techniques to minimize certain things.

And then sometimes in some cases you would use a centralized data platform. To remove some of the PII and it's centralized. So therefore it's a kind of a trusted third party but the challenge with all of that is that you, as you do more and more stuff to the data, you're actually minimizing the utility or reducing that utility for the data as well.

So on one side of a continuum, you are. You you're addressing all of these risks, but on the other side, you're actually reducing the utility. And it feels like you're constantly trading off these things against each other as if they're mutually exclusive to try to get to some sort of middle ground where it's acceptable based on the risk controls of the organization and the cha the challenge there is that if you think that's.

Hard enough, this all takes time, and you end up killing deals. But then if you add to it the in these regulated industries, there's a real reluctance to let data, leave an organization. So if you're dealing with raw data organizations, don't allow the. The raw data to leave their

control the, their environment to go to another you know, you naturally got information, security requirements as well, and a kind of a real desire to protect the data and transit at rest.

And also in use that kind of lived those challenges. And it was a bit of a slog to be honest, a bit of a slog. And then that's how I came to discover privacy enhancing technologies, which I think as, as I was doing some work with the C S R O. One of their teams that was in the accelerator, was looking at homomorphic encryption and looking at secure multi-party computation.

And so I suppose having, having realized those technologies and what you can actually do with those technologies, I how do I put it? It's to be able to do analysis on data while it remains encrypted and also to potentially do analysis on data while it remains encrypted without ever having to move that data from any individual.

Company's environment. Really opened my eyes. I suppose having seen, seeing what data 61 we're doing and looking to commercialize these technologies, having seen the, the possible applications of these technologies in everything from detecting illicit money flows in financial services through to, thinking back to the sort of impediments that I had been facing with almost every single data share between organizations.

Whether it be bilateral or multi later, I just saw so many potential solves for those problems. So I, I, so I got quite excited and bitten by the homomorphic encryption bug, so to speak. And so really, I was asked to step in. Into this project or venture within data 61 to help them spin it out, help them commercialize this tech.

And so I've been quite active in that ad advocacy piece. So I've been involved in the standardization efforts of homomorphic encryption. I've also been involved in the early days. As, as the MPC Alliance, I did raise to the Australian Senate here. It really came off the back of a what was, what happened in Australia,

there was an Australian data matching bill. That was being proposed at the time. And that was really with the objective of reducing fraudulent Medicare claims. So the way the government were structuring things is that Medicare is you know, our centralized body that kind of administers you know, healthcare and that sort of thing.

There, there was potentially 600 million worth of fraudulent claims that they wanted to get to the bottom of and the way that they were proposing to do that was to get, the data from, I think, six or seven other federal state bodies and centralize all of that data in a single place.

Very sensitive data. No, how there ma massive partners. And you know that whole centralization of data The way that it was the way that the whole, bill was being drafted,

was prescribing the movement of data. It was all based on raw data. It was all going to a single place, and it's given it to us all, give us all the powers with it.

And then we'll run analysis on it. And if we find fraudulent claims, then we're gonna tap on the shoulder kind of thing. So really use that as an opportunity here in Australia actually to collaborate with gal white, Inc. So they're us based cybersecurity firm, great pedigree.

In home or encryption, secure multipart computation other privacy, enhanced technologies really use an opportunity to showcase what else is going on in the world. Let's broaden the horizons here. There, there are lots of countries around the world and age government agencies within those countries around the world that are embracing these technologies for evidence based policy doing things in a way a that allow the richness of that analysis on data without having to actually physically move that data without having to risk citizens.

You know, security citizen data and also the privacy. So we, so we put a lot to go together there. And unfortunately it really fell in deaf ears here in Australia. There was, we did a lot of campaigning and advocacy work, and we listed some enlisted, some others.

But through that campaigning work you know, met with a few ministers and senators here in Australia. And that was the background to then. Being asked to put some stuff to the Australian Senate as part of their FinTech and RegTech inquiry here on how could we use some of these technologies in a FinTech, RegTech, financial services setting?

How could it be used to generate another industry or, generate do it from a, from an export perspective. So from a, from a technology export perspective Yeah.

**Eric:** And what happened to that Medicare bill, or I call it Medicare. How, what happened to the fraudulent medical bill?

**Alistair:** Unfortunately the bill was passed so now there, there, it's entrained in legislation that these various. Agencies are forced to share that data. And we had, of that, we still had ongoing dialogue with the federal department of health, unfortunately.

And I think this is a challenge, you know, really broadly speaking, a lot of these government agencies, they're trying to solve the problem in front of them. If that makes sense. They're not necessarily aware of some of these cutting edge technologies that are, maybe a step away or two steps away in the future from what is absolutely mainstream right now.

And I really do understand it from their perspective, which is they're trying to solve an immediate problem

**Eric:** the way that it's always been done, but it's not accounting for the fact that the amount of data is growing exponentially.

**Alistair:** Exactly. And I think. So there's a real lack of awareness on, on, you know, what some of these technologies are gonna, they're gonna soon be mainstream.

They're still a couple years away before that's the case I feel, but to not even be aware of them to, and then to almost draft legislation in a way that, that, as I say, prescribes a movement, data prescribes the use of raw data. You're accidentally prescribing things in, which, leads to undesirable situations,

right.

**Eric:** The honey pot effect and in the context of, and just to remain with that example for a bit, the, a secure multi-party computation type of architecture might have had each of the agencies retaining their data and potentially performing computations, which designed to produce a result that would be indicative of a red flag, that to further investigate.

Then there would also be even now with the data centralized, they could homomorphic encrypt it and still gain those benefits. Of course, that would require a fair amount of upgrading. Like I think it's a very interesting example and I'd like to explore it more because you had firsthand experience with it.

**Alistair:** It almost flows in the way that which countries are more mature in evidence based policy which countries are more mature in kind of data privacy, but then beyond that its which agencies within which country are more mature in their thinking of bad about how they undertake data sharing partnerships with the private sector or into governmental

partnerships, and sometimes it comes down to the people that are in those agencies, frankly, to, to give to give you a sense, the Australian, it certainly felt for the conversations that these, the Australian federal department of health here were a long way off in terms of their understanding a long way off in terms of their maturity around the issues and risks that are thrown up.

By raw data by sharing data and just, you know, it's also very clear through that example, by the way, that there were a lot of politics at play you know, control between agencies and that sort of thing. But, but, but there are some examples, I'd say the likes of I, I M D a in Singapore, right? So AR in Infocom media development authority and their kind of privacy data, I'm trying to remember the exact number, but their privacy.

They've got a privacy in data commission and as part of some of the work that they do, they work with the private sector. So they'll do hackathons, they'll do a variety of different things to stimulate closer, closer ties between industry and also government. And as part of what part of that, they've got a safe data sharing framework.

So they are actually. Actively go out and promote ways to undertake some of these data shares for both social good, but also a private sector benefit. And as part of that, they explicitly call out the use of homomorphic encryption, secure multiparty computation, as ways to undertake these data shares.

Similarly, I mentioned the OS track example here. So that's obviously an agency that sees the benefit and it's a three it's a 3 trillion or problem globally around anti money laundering, money flow. So definitely the carrots there, but then you can also look at their counterparties.

In the UK, for example. So the FCA are also pretty active in both the promotion of privacy asset technologies, but also then trying to understand more and more about, about that and what the applicability is in Fs, financial services. Sorry. And then, I feel we're seeing more of that in the us come through as well, both in the maturity of data, privacy laws, like for example, what's going on in California.

But then there are, I think it's the FTC in the us, or also looking at more privacy announcing technologies. How can they be used? Again, it, it feels like that fin crime and anti-money laundering use case is the one that kind of is the big carrot for them. And so I suppose for me, it's more about, I think there's still a way to go in terms of the advocacy.

And I, and I think, and it's a complicated thing to answer because. I think it comes from a combination of factors. It comes from more and more, geographies around the world are coming under more intense privacy legislation. So you've got a greater drive from consumers, but also regulators to get what more privacy loyal in there to actually then be more, which is more restrictive for private sector are on what they can and can't do with that data.

And what's expected of them, frankly. You've also got a growing. Awareness, know from tech vendors in the space around what the opportunities are, those, those earlier use cases or the, a real thing that kind of helped to be the tide that lifts all ships, right? So you can point to those proof points.

And then you've got those pockets of reg regulators investing in the space. Internationally that then can be pointed to as use cases again, to have that kind of groundswell. And I think Frank, frankly the likes of the privacy enhancing technology summit, bringing a lot of these people together also helps.

To generate that awareness and bring together the people who know and who are subject matter experts in the domain, versus those who have industry problems such that there can be that gelling of the, these are those killer use cases. And frankly, I think it's gotta be quite a few things that need to come together before this becomes mass market.

Um, But, but I do think from being in the space for the last few years, we are at a point now where it is very close to a breakout, if that makes sense, specifically, I'd say MPC probably is ahead of he in terms of that in a breakout. But, but whether it's just even the general awareness of privacy intensive technologies, I think is growing for.

**Eric:** Yeah I think I was shocked that, um, the NBC Alliance, about a, you when I first started exploring homomorphic encryption you know, more heavily, in the fall 2019 the NPC Alliance was, the head. It wasn't the same composition that it was today. It was hardcore research organizations.

It was like duality. It was like in Vail, I think it was inferring a bunch of others, but there were a handful. And then I looked at the most recent list of NPC Alliance members. It's like this whole Z KP digital asset crowd just descended on its. I think it makes up like half the membership and that certainly helps because when you have that kind of interest flowing into it you know, it certainly a rising tide lifts, all boats.

Sticking with the privacy enhancing technology summit cuz I'm glad you brought that up. So you've been very involved in I guess the privacy enhancing technology summits that have been in Europe and then there's also the privacy enhancing technology summit. That's gonna be hitting The us first one in Boston May 18th, 19th.

So that's how Alistair and I were introduced through, um, through the crew that's doing that. That's a privacy enhancing technology. Someone will drop it in the show notes check it out be bringing together a lot of experts, some from the down under as well to talk about privacy enhancing technologies.

**Alistair:** There, there

are a few, I look, and I think, and as I mentioned before that I really do think that the team had done a great job in helping to bring together. People who are so world experts, but also those who are looking to explore the space more. And I think it, it really does help to lift, lift to be that tie that lifts all ships and bring people together.

**Eric:** Yeah. And it's interesting. You talk about like different countries and regions who have approached privacy enhancing technologies. And again, particularly around money laundering, risks you know, you've seen the FCA do their technology sprints. You've seen the New York department NYS DFS, New York state department of financial services.

They did a number of tech sprints, including with infer who, I think you van partnered with I think on, on certain proposals in Australia. Um, and you know, I remember stumbling upon on all these tech sprints that were lined up at N Y S D F S. And it was really. Quite something like breaking up like individuals coming, working across companies to just, and maybe working on more than one tech sprints, but each segmented from one, one

another to Devis these sort of strawman solutions from which some of them have actually gone on to actually build some businesses around.

Those tech sprints can be you know, I think it advances the whole privacy enhancing technology. Solution set so much more when they're engaging in that way. And then they're getting real time feedback from the regulators. And even sometimes the regulators are part of the team helping to create it, which I just think is which I think is awesome.

Um, um, rotating a little bit to open banking near and dear to your heart. What is open banking?

**Alistair:** Yeah, sure thing. So open banking, and, and it depends on the jurisdiction, but it can either be regulator driven or market driven, but it's essentially allowing consumers to get access to the data that they, that a bank or another financial institution holds on them such that they can then give that to a third party.

Which could be another bank or, another sort of a, to FinTech and really how that's come about is that, in, in the EU, it started off as a payment services directive two which was really predominantly a brand payments and helping people to get rid of merchant fees and do account to account payments.

Then the UK's implementation of that was really more about current accounts and driving more competition, actually into the nine largest banks in the UK, the CMA nine that are otherwise called. And then in, in various other jurisdictions, it's been a band competition and consumer choice and kind of innovation in the economy, certainly in Australia open banking.

And the thing called the consumer data right here are used interchangeably, but really what it is here is the consumer data, is aimed to be an economy-wide data, it allows consumers to be able to take the data from someone who's holding it on them to be able to provide that to somebody else where they see there's value in that kind of exchange.

And it is intended to be, as I say, economy-wide bank the banking part or financial service is the first vertical of that kind of consumer data. So the term is used a little interchangeably in Australia. Open banking is the first four array, so that the banks, which then expanded into energy telco.

And then other financial services providers like insurance, for example. But I think the thing is important to call out is open banking while it is happening in some of these jurisdictions is actually, it's a global phenomenon. So it's happening, around, around the world.

It's happening in Latin America, Mexico is quite within, within, at time. They're. Some of the most, most proactive and they've passed a law 2018, but then in the us, it's been more

market driven, so to speak. So not having the regulatory framework around it that feels like it might be changing in the next little while.

So that's the background into what open banking is, but I think what might also just be worth at is why does it matter to a consumer, right? Because I think within open banking, there's a real, there's a real tendency to think about what it means to a financial institution, but that's not actually the reason why it's been regulated in any jurisdiction whatsoever in, it's actually about consumer choice, transparency, driving competition into markets.

So driving competition specifically into financial services. And it's really about being able to give consumers the ability to get, a better offer and to switch banks and, and to overcome some of that inertia really. And so that's how it's come about. And so propositions include everything from, getting a better rate on a, on a home loan, getting a better rate on a personal loan, a credit card through to just various comparison apps and being able to switch energy providers.

Switch telco providers, but then you're also seeing other sort of propositions emerge where people can actually get a, get a recommended rate on a home loan, but actually then be able to switch and get an approval on a home loan within seconds.

And then all of the sort of customer onboardings taken care of based on the data that's been shared. So you're seeing some real some really interesting propositions that come at. I'd also say that open banking is probably more the guardrails and framework. For some of those for some of those data shares, so what you can share, what you can share what, what are the sort of rules around it?

**Eric:** And it's interesting. So as a consumer in the us, and maybe again, maybe my experience is limited. Does the average consumer under, do they actually experience like an open banking platform, or does it happen more on the back end?

Is there,

**Alistair:** yeah. So how, and it's a great, it's a great, it's a great pickup actually. So how in the us and other markets where it's not regulated, how they typically experience it is I'm trying to think of a kind of a specific use case. Let's say it's a bank or a non-bank lender offering a fantastic rate on a home loan or a mortgage in order to get that rate or a personalized, they'll ask they'll prompt for, Hey, can you give us access to, the data that you're, that. From, your current bank, we want access to how you're spending your money, your assets, liabilities, your transactional data stuff that is then done in the backend using someone like Yolie or Plaid in the us where that is using a thing called screen scraping.

So a technology called screens scraping, and essentially just drives the screen, rather drives the browser or pulls it down it at via API, get sent. And, and, and, to, to the acquiring bank,

so to speak. And so it's very seamless to a consumer. There's naturally an apart from the fact that it's clunky and apart from the fact that it's you know, it.

It sometimes breaches the terms and conditions of, of, um, of the bank, for example, that you're coming, and you're giving your username and password to somebody to come and take the data from the screen. It's it also it's a really clunky kind of technical solution and it does not have the right data, privacy guardrails.

Or InfoSec kind of guard rails around it. And it, and it's implemented in different ways. And some banks block it, actively. Other banks are they, they let it go and others are just more in that that watch where they wanna know exactly who's doing what who's hitting, who's giving their credentials away.

Yeah. So it's, that's, it's it is seamless to a consumer by and large, but it's happening in the background. All right. And

**Eric:** I, I think, um, most people in the us at least have probably experienced plaid in some way for shape or form given a consent. Um, and in, in an open banking system, you've noted some of the clunky, the, some of the problems that maybe aren't the best for privacy, what pet technologies map particularly well to open banking solutions.

**Alistair:** I think, yeah and I think the other thing that's an interesting one is almost a framing of open banking. So that's the kind of regulator market driven approach. But if you think about the pressure that's put on existing financial services companies, where. Open banking is either regulated or it's market driven.

You've got consumers able to get that transparency and choice of being able to bring that data to somebody else, and there's a real potential threat, competitive threat to some of these organizations. The other side to it really is that. For a long time, and this may be a controversial comment, for a long time,

a lot of these large financial services companies haven't done very much or enough with the data that they've currently they've been sitting on. So as part of that, there's a, there's an increasing =desire to do more with that data. There's an increasing desire to deliver more personal as propositions to consumers.

There's a desire. To work through data partnerships with other companies in adjacent markets to, to offer that value and personalize. And so that's the framing. And so to undertake that those data shares there's a real, demand growing demand for the likes of HE

secure MPC secure MPC works really well, certainly when there's multi later partnerships. Um, and you know, for example, if you can have a loyalty, a bank working with a loyalty

company to not only drive greater cross sell for, especially if it's a loyalty company attached to a, an airline is actually being able to drive.

Greater cross sale of credit cards that have loyalty points attached to them. But what are those personalized offers that we can then put to someone who is a frequent flyer now that we can give that the orders have opened? You know, and then there's other propositions that are um, which sit along alongside open banking.

So some of the data comes through an open banking regime, but what about the other data that we have? That's not mandated to be shared. Can we set something up using homomorphic encryption where? We, we can provide an insight to a FinTech that's closer to us such that they can provide a proposition and almost that combination of closed ecosystem alongside that open ecosystem.

And so there's growing. Certainly in Australia, there are a number of banks here that are investing heavily in secure MPC hiring. And he And, and really looking almost to see what can be done in delivering some of these consumer propositions using the data that they have that sits outside of an open banking regime.

So very symbiotic, is the way that it's been looked at.

**Eric:** Yeah. And I guess there's sort of two ways of looking at it. One is to try to enhance the overall customer experience with more personalized services or offers. And then the other one is thinking about almost marketing partnerships.

**Alistair:** Yeah, absolutely. Yeah, and it's not just in Australia cause the, is, there's definitely banks in the UK, which are further along the journey in open banking that are, investigating this space and, and are using. E to even work with each other to you know, what are those things that we can do with consumers that are that that, that they can, that can't be done through open banking and by the way that's also almost touch on another theme of how open banking has um, has come about.

Is it open banking and almost every jurisdiction has come about because regulators have tried time and time again, to get banks to be more competitive? And to do more things, to make it easier for consumers to switch away. And it's it, in almost every situation where banks haven't done that and got together, that's when the regulators have stepped in and said okay, so here's a regulator here here's a regulatory regime have forced this. So I'm certainly seeing some of those essence being learned and actually, banks and other financial services companies going well, how do we now use these technologies to work together? Because we now certainly see the north star of where this all sort of heads, which is towards, greater openness, transparency data, almost being a proxy for money.

In, in, in, in these sorts of setups too.

**Eric:** Yeah. And certainly like data portability, turning into an opportunity. You know, that's certainly, we're just at the beginning of that, right?

**Alistair:** Oh, a hundred percent. A hundred percent.

**Eric:** And, and do you think data portability is an opportunity that the obvious use case is open banking?

Or do you see other opportunities that may be tangential or related that might be equally compelling or more compelling?

**Alistair:** Well, the, the other, the other way to look at it is da data portability and sharing data. We've been as consumers. We've been doing it for a long time. So we've been doing it.

With likes of Facebook and others for a very long time. Now, this is more about the kind of the guardrails that are being put around it to, to make it safe. And, for example in, in Australia, you've got the right to delete. So you can go to the bank and say, look, you've got my data through the consumer data, right regime.

I now want you to delete that data on me and they have to and so they're legally obliged and they have to then You know, it's not as strong as GDPR, which is the right to forget. So forget you, we knew kind of thing. I, I think so. So data portability has had a lot of opportunity for a long time.

I just think it accelerates whenever there's a regular pure regime that makes it really, it actually makes it safe to share that data. And as a, and as a consumer, safeguards are in place to, to be able to do that. Um, But I think it also within open banking almost needs to hit a tipping point where there's enough consumer propositions in markets.

But to answer your question about some of the other areas and other, areas where data sharing can deliver value. I really do think in, in some of those either public sector, data shares or combinations of public private sector data shares, there, there's an awful lot of untapped opportunity there where.

Before some of the impediments that I've certainly experienced. And I mentioned earlier, would've blocked either evidence based policy decisions or, or, or things we just cannot detect patterns of fraud, that there are now the opportunities to safely and without needing to move the data and having to go and acquire all of that data and bring it to you.

You can actually bring the algorithm to data. Where it currently resides. Naturally healthcare is another area which is, um, has so much opportunity. I

**Eric:** know we talked a little bit about jurisdictions and it's difficult, it's dependent on jurisdictions, but where do you see pets being, which jurisdictions do you think are most prime for or the monetization of privacy enhancing technologies?

Like the commercial use case? Not so much the public one.

**Alistair:** Certainly in Australia, our major banks, as I say, at least two of our major banks are actively looking at ways to not only spin up new propositions that are underpinned by privacy enhancing technologies but also way, potentially new ventures in the space.

So there's a real kind of appetite to see. To see the opportunity for consented data share consumer consented data share. I think jurisdictionally, the us would be pretty far ahead when it comes to some of the tech giants, right? So you've got FA Facebook very active or meta now. So very actively hiring in the space and secure NPC and actually also and he as well.

And, and, looking at their kind of private lift measurement. PE pieces for their ads, is underpinned by a lot of NPC technologies. You've got Amazon and through their Alexa fund, looking at investigation of NPC for kind of previously preserving analysis over voice.

And they've made recent investments, right? Like with likes of info. And I'd also say that you look at what the likes of you know, Microsoft have been. Very active in the space OFE but also MPC for quite some time. IBM Intel. I really think the us will be the first market where a lot of this stuff, in fact, it's already there, it's already behind the scenes, not necessarily being, being lauded as an MPC solution or a solution it's embedded, it's fully embedded. I'd also say that in the intelligence community, it would be north America. Generally. That would be well ahead with the use of some of these technologies in, in In intelligence settings as well.

Yes, I'm in Australia. Yes, the UK and the rest of Europe. But definitely the us they'll probably be leading the way there. And so I suppose if I was, forced to say one geography or one jurisdiction where I thought would lead the way it would be the us. But what about,

**Eric:** You know, just working across competitors, working you know, horizontally, so where you have potential competitors sharing information like for research and then just, leveraging their individual data pools, potentially, presumably with secure multi-part computation, not.

E and then, benefiting that way. Have you worked with those kinds of initiatives and seen how they develop and yeah, so?

**Alistair:** certainly the one that jumps out is around insurance, um, being able to identify potential insurance and fraudulent claims between I insurers certainly here in Australia and I know it's happened elsewhere around the world.

Unfortunately this one didn't get off the ground, but it was one where it got quite. Into kind of you know, quite well into the execution. And it was really about how do we identify those people who have, multiple car insurance policies across different insurers who traditionally don't share data with each other for a bunch of reasons once competitive, the other ones, actually, it's a regulatory, there's a set of regulatory challenges is how do we then.

If that person goes and, crashes, the car makes a claim against two insurers. How do we make sure in that this double dip scenario that's actually, we know about that and that it's fraudulent so that we don't actually pay out twice? And so really getting those insurers together to you know, agree the framework, look at some of the technologies to be able to apply.

I, this was using some of the privacy preserving technology. So specifically some But it was actually more using blockchain solution, actually. And, and I this, this falls down, not because of the strength of the merits of the technology, but more the sheer difficulties in orchestrating four to five large organizations to all agree and all come together and all to trust one another enough and all to execute, to get.

So that's how that falls down which, is probably one of the challenges that I see about. Multi-part computation adoption specifically is that if you need multiple participants to generate value, it's actually, how do you get those multiple participants together to actually not only agree on the solution, but to participate together.

And then I think the other challenge as well is from a pure sales perspective. How do you have to go off and sell to each one of those participants to, to get that, to get that to actually happen. And I think, and I think actually you probably heard Kevin McCarthy from infer, say something relatively similar in the past.

But I think, yeah so I don't see that as specifically a technology challenge, as more as it is a kind of getting multiple participants together to execute

**Eric:** together. It seems like going into 22, we're seeing more privacy enhancing technologies find a way into digital assets. Like I mentioned about the NPC Alliance it also feels it's attracting more venture dollars.

What are you seeing in Australia? Is it driving more venture investment than is it escalating leveling off still yet to grow?

**Alistair:** So definitely to grow the privacy announcing technology, certainly in Australia, I'd say from a venture perspective are far early on that kind of awareness curve slash the actively investing side of things.

I, I think, globally, The likes of the west coast, us east coast, us funds that they're far more active in this space. And I'm certainly seeing a greater appetite in investment for investment there. I'm also seeing in Europe, frankly, you've got the likes of Enterprise Ireland, which is the export arm of the Irish government and a pretty active sort of seed investor.

They've invested recently into separate Homomorphic encryption secure multi-part computation startups. You naturally have the big tech companies investing directly in this space. But also then through, as through them being LPs and various different funds. And obviously, you got the likes of a teammate in Israel, investing heavily in the space Australia.

I have, I don't, haven't felt that the awareness of the technologies is where I think it needs to be. I also think I, I 'm seeing. More appetite, from the corporate venturing arms hereof, of companies predominantly the sort of financial services side. But, but I do think to your question it, I really feel that 22 is a kind of a potential break breakthrough year.

And there is a lot more money flowing into it. And in fact, some of the startups that I speak to raising series a and series B, they're not having any challenges whatsoever getting a lead. Or indeed, you know, feeling like they're gonna they're gonna fill a ramp, right? It's becoming more and more on people's radars and kind of the money's flowing behind that.

**Eric:** All right.

**Alistair:** Awesome. Eric. Thank you.

**Eric:** Thank you so much. You take care.