**Matthew Todd**
Hi. My name is Matthew Todd, and welcome to Inside the ScaleUp. This is the podcast for founders, and executives in tech, looking to make an impact and learn from their peers within the tech business, we lift the lid on tech businesses, interviewing leaders and following their journey from startup to scale up and beyond covering everything from developing product market fit, funding and fundraising models to value proposition structure and growth marketing. We learn from their journey so that you can understand how they really work, the failures, the successes, the lessons along the way, so that you can take their learnings and apply them within your own startup or scale up and join the ever growing list of high growth UK SaaS businesses. Hey, welcome back to the podcast pleased today to be joined by two co founders on the podcast, which is the first time we've done this, but really excited to hear about the journey and we've got Alan Jones. So an awful Jones cofounders of yo messaging. Good morning. Great to have you here today.

**Alan Jones**
Good morning. Good morning.

**Sarah Norford-Jones**
Hi, thanks for having us.

**Matthew Todd**
No worries, I'm excited to learn about the Yeo Messaging journey and learn more about some of the lessons that you've learned as as well. To kick things off, can both of you give a brief intro to yourself and explain exactly what Yeo Messaging is as well.

**Alan Jones**
My name is Alan Jones. I have been in the tech industry for the last 40 years. Sounds like an age, but it's been a hell of a ride, I can tell you, if you look at the changes in the industry over that time. Yeo Messaging is the fifth startup I've been involved with at the founder level. Yeo is born from the realisation that we're all vulnerable on messaging platforms and social media platforms. We have absolutely zero or had zero control over anything that we had sent. I had a desire to repatriate and control and to be able to control all of my content once it was it actually left, or I'd hit the send button. We'll explain a bit more about that later. But Yeo is all about privacy, confidentiality and control.

**Sarah Norford-Jones**
I am Sarah, I'm one of the cofounders might actually also Alan's daughter. He came to me with the idea of Yeo and wanted my experience from my background is in marketing and advertising. I have worked in that industry for less time than Alan. Obviously, I'm his daughter. So 12 years. I've worked client side and also agency side for brands such as Shelf, Ferrari, Samsung, to name a few. Alan came to me with the idea and wanted my knowledge of where best to position it within the market and how do we make it look nice and feel good and relatable for the industry? So that's my role within Yeo.

**Matthew Todd**

Awesome, thank you sounds really interesting. I'm keen to get into more detail about the what exactly that looks like in practice and how that journey has changed as well. But I guess the first question is, why, why another messaging app, what is missing from the current kind of state of play security, privacy controls that, you know, apps like WhatsApp or other apps are offering to the market.

**Alan Jones**
So basically, every application that is there today, and there are many, and I think we all use probably between one and three of them. You have no control on anything once you hit the send button. It really is send and you rely on trust. So you believe that on in the integrity of the recipient, so no matter what you send, you're in their hands and that backfires on a regular basis. There are no applications today that are lending themselves to protect content, post delivery. That is exactly the the niche and the the need that we're addressing with Yeo.

**Sarah Norford-Jones**
If I can add as well. All of the ones that you listed, and many others they all focus on what happens from point when a message is going from Point A to Point B. So the encryption side of it. So man in the middle attack. What we're doing is actually protecting the message and the content once it's delivered to the device. So it remains in your control once it's even on the device of the recipient.

**Matthew Todd**
I see. What kind of control does it allow you to have over that message, is it simply unsedning it?

**Sarah Norford-Jones**
So we use patented facial recognition or continuous facial recognition. So every message that I send, I can set with the Yeo mode setting, which is the your eyes only setting which means that the recipient has to have their face and only their face in view of the camera of the phone, whilst viewing that that message. So if they try and show somebody else, the message will actually blur. If someone gets the phone and tries to have a look at what you know what they're sending, or what they're receiving, the messages are not visible. So  from a point of view of authentication, authenticated messaging, we are allowing people to send messages and know that is only the person that they're sending it to that can view.

**Matthew Todd**
I see. That sounds like something pretty obvious, but a massive security improvement shift compared to how any messaging app works? You know, as soon as you unlock the device, it's for anyone to see, isn't it?

**Alan Jones**
Yeah, absolutely. The other thing we do is we authenticate the sender, and the recipient. So there's no bad actor, position or capability on Yeo. So usually, you know it's me sending it, you know, who you're receiving from. So that eliminates phishing, cat fishing, grooming, etc. Which is a massive advantage over anything today.

**Matthew Todd**

In terms of use cases, what kind of use cases are you seeing people choose this type of technology for? Legal? Is it for information that is highly confidential in nature? Are there different kind of use cases that you're seeing?

**Sarah Norford-Jones**
That's exactly that. We will get into a background I'm sure of where we kind of started. But right now, what we're really seeing is regulated industrie. Any industry that needs a form of authenticated messaging communication, is dealing with highly sensitive data, or, documents sending, as you said, legal, it's another one. That's really where we're seeing a lot of demand.

**Alan Jones**
And healthcare, of course,

**Matthew Todd**
What kind of health care?

**Alan Jones**
The use case at the moment is the rhinoplasty society. So that's an obvious one, they're dealing with the face at all stages. There's been instances where doctors are using WhatsApp to communicate with clients, patients, which is it's in breach of GDPR, it's in breach of any privacy regulation around the world. Yeo enables them to you have the instances of messaging, but to be able to confidently communicate with highly sensitive personal data at any time, and photos and videos of operations, etc.

**Matthew Todd**
I can certainly imagine a whole number of use cases within medical, but other sectors as well, where that would be extremely desirable by any client or party, having to have those kind of confidential conversations. I know from firsthand experience, you can sometimes feel that data that it shouldn't be private, isn't. I've been inside hospitals, and had nurses and other health care professionals writing patient notes on the back of a napkin and handing it to other staff to type into a computer system. The whole information exchange just felt completely non technical, but also non private.

**Alan Jones**
It's absolutely true. And in those situations under Yeo you would be able to do a voice recording, so send a voice message. But that could also be sent in what we customize Yeo mode. So you know that the person receiving has to be the one that actually holding the device at any stage.

**Matthew Todd**
So when you send message you can choose what that recipient kind of mode is.

**Alan Jones**
Yes, you can. And you can also geofence.

**Sarah Norford-Jones**

I was going to touch on some of the other security features we have, obviously, we've said the patented continuous facial recognition. But we have geofencing, which allows you to lock your message into a particular location and as soon as you leave that geofence, the message is no longer available. So if it is a hospital, for instance, you could set your message or your chat feed where the certain person to that hospital location, which is another really good kind of security element when coupled, especially with the authentication.

**Matthew Todd**
I'm sure everybody is aware of very high profile examples of WhatsApp messages, etc. getting out into the open and wrong hands exposed beyond their initial use case.

**Sarah Norford-Jones**
The news helps our argument every single day with some great nuggets, especially the UK government really helps our argument for an need for what we're doing.

**Matthew Todd**
So coming back, what was that initial founding 'why' for Yeo? What was that kind of process like to take it from idea to actually inception?

**Alan Jones**
It's quite interesting, actually. Because the first thing I did was, look to prove the key technology. The first thing was was, well, this is a great idea, but is it practical? Will it really work? Can you actually get the camera on the phone to come on and off on a in a continuous fashion over a period of time without draining the battery? How do you optimize performance over degradation of power? So that's the first thing we did to make sure that it was practical, because often you have a great idea, but you just can't implement it there are barriers, technical barriers, etc.

**Alan Jones**
The next thing when we proved that that could work was to write the intellectual property. To sit down and propably properly flowchart, the use case, the and look for the novelty of that use case in order to write the intellectual property. So before we even registered the company, we had gone through that paper exercise in order to do that.

**Matthew Todd**
Was that because you saw IP protection as something critical to the business?

**Alan Jones**
I think IP protection is a hurdle that you definitely want to have. It demonstrates that you have applied the appropriate due diligence to the technical solution. To actually put it down on paper and go over it troubleshooted take on constructive criticism for it and hone your proposition going forward.

**Matthew Todd**
So is that IP protected? Just in the UK? Is that more more global than that?

**Alan Jones**
No, we registered the patents in the UK and the USA, and also in Europe. So we've got a European patened in process. We have a US patent granted, and the UK patent is granted. They were our initial target markets and the easiest to uphold, as far as patents are concerned. There's a lot more respect for patented material within the within those territories.

**Matthew Todd**
What was the what was the initial product? What was the initial use case or launch of that?

**Sarah Norford-Jones**
Well, we our plan was always to be a consumer messaging platform. We did a lot of market research. We did a YouGov survey which we got got some great feedback and data about consumer usage, and the fact that they wanted to use a messaging application that protected their content and privacy, and would be happy to pay for it. When that came into practice, and we launched our consumer application, we actually gave the first 2000 users the year free. Then after the 2000 users, I think we gave one month free trial. Then there was the paywall bit but we noticed a significant drop off of consumer users as soon as they hit the payroll. That was even before they had their one month free. So we had to kind of reevaluate and think, okay, maybe the data that we went out and, and got isn't actually working isn't isn't the truth. So, at that time, we had been accepted on to an accelerator program called Cylon, which was really a great introduction for us to many, many businesses, a lot of them regulated industry businesses, and kind of the cybersecurity world as such. We've made a lot of great connections with mentors and partners and potential investors. All of them were demanding the use for what we had and our technology within their business. Which is when we decided as a company that we wanted to actually shift and pivot what we were doing from consumer to b2b. We took the app, redesigned, it redeveloped a lot of the things that needed to be done for it to be appropriate for business use. That is what we have today, it is now you know, we're now focused on our partnerships, and our clients within business. Health care was one that we spoke about, we also now offer a white label solution of our applications. So companies and businesses can literally take what we have, redesign or integrate our solution within the existing infrastructure.

**Matthew Todd**
Interesting. Yeah, I'd love to get into more, more detail about that. But what do you think the barrier was? Do you think it's just too many free messaging apps and people not really willing to pay for the benefits?

**Sarah Norford-Jones**
I think that and I also think that so many people, they've already given away their privacy. They know that they've shared on Facebook for the last 10 to 15 years. I feel like they've they've already done the damage. So when it came to it, they almost were like, 'Ah, it's done now'.

**Alan Jones**
Personally, I think things are changing. There's been so much more awareness, through through journalists and the government initiatives, etc, to make people realize the danger of being totally open on social media, etc. We've had situations where people could be monitored on Facebook as to where

they were, while somebody's knocking off their house, etc. There's other situations like, young mothers being very conscientious now about posting pictures of their children. Dozens and dozens of examples, even down to the glorious Matt Hancock recently. People are becoming aware of the ramifications of just being frivolous with their their privacy on social media. So I think it's changing. But but when we first launched, there was this tendency to first all your friends are already on one of these platforms. So you either move on mass, or you have a leg into camps all the time. That cross pollination isn't there even today, which makes it difficult, and the legacy contacts and so on, again, unless you you move on mass, new products like ours, are going to be slow to take over in markets and will be used for specific cases, like someone doing a financial transaction, somebody wanting to share secret information between themselves. Organizer, surprise party, etc. a lot of that stuff starts to go to Yeo. I'm seeing more people using it for finance and discussion of personal medical data.

**Matthew Todd**
Yeah, it makes a lot of sense. There's definitely that network effect, like you say, people moving on mass, but I agree that people are becoming more aware of certainly what they share on social media or some people but you still see people, you know, on the Facebook feed, or whatever it may be certainly compromising what should be personal identity kind of information. Whether it's I'm going to be away from the house type of posts, like you mentioned, all these kind of quizzes and polls and tests that they do what they don't realize they're giving away all this information that could be used in the wrong hands for the wrong purposes.

**Alan Jones**
Well, we've seen it, there are so many cases of people being basically abused online through by blaming information from social media, etc.

**Sarah Norford-Jones**
Or even just, there's a lot of people out there that you wouldn't think, oh, it won't happen to me, or I've got nothing to hide, and then they're the people that will have their whole identity stolen for fraud in some some way, because they've shared pictures and identifying objects within their photographs that they share. We've done a lot of research into this. That's one of our biggest passions and drivers for what we're doing is protecting people.

**Matthew Todd**
I think there's that I've got nothing to hide is what I hear a lot of people saying, I think lately, so people have almost given up on like privacy because they used to like personalized ads on Facebook and everything else that they just kind of accept that. They know everything about me anyway. Sometimes, oh it's scary how they seem to know so much about me like I was stood next to so and so and now I'm seeing adverts related to the things that we were showing. So they almost have defaulted to I can't push back against that anyway. So I may as well.

**Alan Jones**
I think legislation is moving to change that. The latest Privacy Act that's coming through now, I think it will change it. It will hopefully limit the numbers of cold calls that we get.  My poor old mum, she's 88 year old years old and when she gets a call saying somebody, they're so familiar with her, about her,

her electricity, or they call from the bank or whatever. They get confused because they don't come from a background where they're rude to people, they like to hear and take on board what somebody's saying before they make a judgement. But you can just watch her being led down the garden path by some guy who's reportedly going to help her in some way. Meanwhile, they're they're embezzling money from these these vulnerable people all the time.

**Matthew Todd**
Yeah, absolutely. I think, as you say, the information that they can have access to just makes it so much more convincing, doesn't it? My parents have had calls that they have been suspicious of and sometimes it can genuinely be hard to tell whether they were or were not genuine because of that, that information that they had and the way they came across.

**Alan Jones**
What these people do is that they take the information that from social media, eventually they end up with your phone number, and bingo, away they go. They know who you are, where you visit, who your relationship's are with etc. and they can pose from a position of familiarity, which leads you into a false sense of security and bingo, suddenly there's 1000 pounds gone from your account or whatever.

**Matthew Todd**
Going back to the the kind of case for secure messaging, whilst technology has done clearly a lot of very, very good things, a lot of innovations, that hasn't really been to many proven ways to securely communicate information. So you know, you deal with any number of other businesses or parties, you pay them for services, you need to send them money, you need to take money for things that you sell, or whatever it may be. Quite often people still will just resort to an email, or I need you to email me a scan of your passport, why I don't really think I should be sending that to you on email. But what choice do you have if that, you know, most common method is is the fallback?

**Alan Jones**
Well, we think within five years, people will say, just Yeo it to me. At that stage, you will automatically have a link from your email package or your other messaging application, where you will be able to Yeo a document. It would require facial recognition in order to open it. I mean, on a continuous basis in the Yeo mode. We're already are doing that with Slack. We will implement it with Microsoft Teams and other applications. So people can actually choose when they want to send a secured document or secured message and use our, our technology to do that.

**Matthew Todd**
Yeah, absolutely. I'm already thinking about numerous conversations, people like accountants, etc, that I wish had happened would happen on Yeo, to be perfectly honest. I know people that have had their accountants that outsource work and things like this, and there have been data breaches, and they've almost lost their entire business, because their registration details have effectively move to a different person. It's been months and months of pain, trying to access all of their accounts and act as an adjustment business.

**Alan Jones**

Well, there are so many day to day activities that we have, or uses use cases like new insurance. Say you're trying to ensure high value art or jewelry. The way they conduct the business today is 'oh, send me through the receipts'. You send through receipts or valuation certificates via email and could be messaging. So these are totally open sources of information. So I went to a very well known insurer that you're asking me to send all of this information through to so where's it stored? He said, 'I can refer you to our tech team' . I just suddenly thought, well, if I was a thief basically, then what I would do is go to an insurance company like yours and scan a file so I know, who had what jewelry in the local area, and what the safes work because you also get the information on the safe. So you'd have all of that information, you just pinpoint them and away you go.

**Sarah Norford-Jones**
So if there's any thieves listening to this podcast, there we go.

**Alan Jones**
If they were that they were secured, and they were secured with continuous facial recognition, then nobody could get them they would not be decrypted in any easy way. It would be secured. Then there's the medical situation where you go to your GP you have some tests run, etc. and they then require you to go back in to pick up a letter to give you the results because you don't want to send them by mail and or a secured portal. A secure portal means you get an email to say you should go to a portal in order to retrieve information. But they don't know it's you. They have no idea.

**Sarah Norford-Jones**
Also from a user perspective, it's just a pain to have to remember all these different passwords to enter into a secure portal, they put you through different hoops and loops to get there? Once you're there, they're so clunky and old fashioned. It's not at that instant messaging that we're now used to where you receive something. How much nicer would it be from a user perspective to have that secure portal, but always as an inbox on your device that you can access all the time, and you can have messages come through from bank, health care, insurance, accountants all in one place. So that's kind of our our biggest vision for Yeo is always to be the secured inbox on your device. Instead of multiple secure portals that you must enter.

**Matthew Todd**
These secure portals aren't actually as secure as, as people would want them to be. I can certainly see how with Yeo, you're doing both. You're improving the security, you're improving that control by making sure it's not just when I send it to you was that delivery secure, but it's, it's about who is reading it, and what are they reading, etc.  I'm wondering with such a clear benefit such a broad number of use cases, and I wish every company I had to engage with was was now using Yeo, how do you start to commercialize this? Are you kind of going use case by use case? How have you tackled that?

**Alan Jones**
We have what we call inbound traction right now, which is companies coming to us and saying we have to use your product. We have people like the rhinoplasty society where they basically said, look, we've got to be using this, we have a problem, you are the answer. We've had situations with, there's a digital content network that again, came to us and we have to use your application, it eliminates phishing, we

need a secure platform for payments and for financial arrangements. We've had solicitors to come to us a group of UK solicitors and again saying we have an issue with sending restricted information and our clients are sending information on WhatsApp. We need to eliminate that, we need a secured, auditable platform in order to in order to enable this to happen. So that's what we call inbound traction. Outbound wise, what we're doing is we are making our solution cloud agnostic. Which means it will run on an AWS platform and a Google platform etc. The next thing we're doing is developing the application program as interfaces. So it can be easily integrated with common business management applications. Therefore, the communication aspect becomes part of what you do every day. Not an addition to it, it's integrated within it which makes it much easier to use. At that point, which will be early summer this year, we will then start a sales drive to address all regulated industry, then we will we will pick them off with we will start off with private medical practice because it's the lower bar lower hurdle to get into. We will go into wealth management and small private banks, insurance from the broker side initially, and look at tackling other verticals that require highly confidential, private confidential and auditable communication in any way.

**Matthew Todd**
Sounds like you certainly have a very, very solid, well, well thought out approach of, of hitting the those areas.

**Sarah Norford-Jones**
One thing to also mention, we have our consumer app, it is our free application that is available on the App Store and on Google Play Store. We do minimal marketing in terms of driving downloads for that. But we use that as a really good kind of testbed for features and things that we're integrating within the app. So I just thought that would be worthwhile mentioning, because obviously, although we are targeting businesses, we do need consumer users as they will be the client or the patients or the users for the business use cases.

**Matthew Todd**
I think that's really interesting, actually, because I know a lot of SaaS businesses that have made that transition from b2c to a b2b model, because they realize that it seems like the cost of acquisition and b2c and the scale that they need, are just too high to make that revenue generating business sustaining. So therefore, they go to b2b whether there are bigger opportunities. But I think it's really interesting to keep that b2c elements, although not where the drivers still going to get those lessons and to get a bit of that network effect as well.

**Sarah Norford-Jones**
Exactly. Without any paid marketing or any real drive in that in that area, we are still seeing daily downloads, which is pretty nice to see. It's scaling slowly and organically alongside our sales push for business.

**Matthew Todd**
That's really interesting to see. A lot of founders listening to this that have been thinking about or potentially made that that switch should possibly then consider whether it is worth keeping that b2c element as a sustainable kind of strand to their business, but I think for some types of products,

keeping the b2c going with a slow but steady growth could still drive platform growth, ultimately, and grow into other use cases as well, I imagine.

**Alan Jones**
I used to think the data reform bill will help because people have to then be more conscious of the control of private media, how they communicate with consumers, etc. Again, that puts more and more emphasis for companies to incorporate services like Yeo, into their their arsenal of communication.

**Matthew Todd**
Yeah, I guess that legislation is obviously going to open up a lot of doors, because companies will have to adopt more secure communication practices. But I suppose in terms of awareness, building as as well, it's going to do a good job for you in terms of making people more aware of the problems with current solutions that are out there.

**Alan Jones**
I think it will go a long way. It will go a long way to to eliminate these calls you get every five minutes from somebody trying to either sell you something called con you out of something. Because they are clamping down heavily on that unsolicited calls, etc. Although it will be really interesting to see how they can police it.

**Matthew Todd**
I guess that's part of the problem as well as is Yeah. How is any of that even going to be enforced?

**Alan Jones**
That the next stage, isn't it? It's a bit like us going back to the very beginning. Well, let's see whether it works first of all, before we implement it. If only government was the same, instead of somebody writing up some new legislation thinking this is a great idea. Is it practical? Can it be enforced?

**Matthew Todd**
On that note of that legislation of online safety, I know a number of messaging app creators have been pretty critical of some of their proposals because they believe it will weaken security by essentially enforcing the client side, the apps must report certain types of content and enable certain types of government monitoring for you know, law enforcement, terrorism, all of those purposes. What's your your view on that?

**Alan Jones**
There's been a lot of rumors and comments about different companies saying they will pull out of the UK because if we restrict encryption. There has been, I think, feedback from again, other organizations concerned about the the monitoring of data. I believe that the data I generate is mine. As long as I can retain ownership of that good control of that, I'm happy. I sincerely believe, with the way that we have designed Yeo, that that enforces, and underlines my personal goals, which is retention, of ownership of your data, protection of your data and control of your data. Therefore, as Yeo messaging, we welcome the changes to the legislatio. I believe that they are forward thinking and I believe provided they can be enforced, will make our lives safer, and go a long way towards making our children's lives safer.

**Matthew Todd**
Effectively, what we're looking at is legislation that is adding more responsibility to organizations that use user generated data, no matter what type of, of data that is, and obviously GDPR, I know, there was a lot of talk about that at the time. You can, you know, argue about whether it's even been effective, and whether people comply with it, it sounds like this is another kind of layer on top, which is actually better suited to help people do communicate and share data these days. So therefore, at least if there is that legislation there. There should be that corporate responsibility to treat customer data appropriately.

**Alan Jones**
I think one thing that they have done in in this legislation is they are removing the requirement for an independent compliance officer. Which some people will say, 'Oh, thank goodness for that I don't have an independent, I don't need to have independent audit'. However, what it is saying is, we will remove that requirement, provided you pay attention to data protection plans to protecting the data of and privacy of your consumers, and provided you stop abusing the data that you're gathering. I think that's a fair trade off. Let's make it easier and let's cut some of the administration. Let's put the onus on companies to be more responsible. There's always going to be those that go around it. So what they've then done is they've increased the amount of fines that can be applied. So it's a different carrot really, isn't it? I think as a business, I was very pleased to cut down on administration. But it's easy to say as a company that was totally focused on privacy. But I think for many, many businesses that will make things easier, provided they respect the data that they have.

**Matthew Todd**
I can certainly see that with these, these changes, and just the general direction, and awareness of, of privacy, that as soon as Yeo does become more widespread in different interactions that people have with the different businesses and services they they use. I can certainly see how there will be an increased expectation then from consumers and businesses in terms of what they expect with the security of their data, how they expect that to be managed. Even just through talking through some of the use cases that you've outlined, I can I immediately see that I'm certainly going to be more aware of these interactions I have with different companies and how insecure they aren't and start to question well hang on, should you really be asking for that data in that way? What are you going to do with it? How long are you going to keep it for? How long? Will you have access to that? And where will that access be? provided?

**Alan Jones**
I think that's very smart to do that, then the more people that do it, the more people the more awareness we create. I think we can reverse this trend, where people basically forfeit their privacy rights in order for payment for free services.

**Matthew Todd**
For Yeo, itself as a platform, where do you see Yeo heading? What' the vision? What is the ambition?

**Alan Jones**

At one stage we said we'd like to see it on everybody's mobile phones and everybody using it. We still have ambition for yo to become the secured inbox on an the trusted vehicle to go to for highly confidential and private communication. If we can achieve that, we would like Yeo to be the acronym for any anything that you want to protect. We hope that in the next five years, that will become the case where people will go to send something and you'll be going whoa, don't do that. Just Yeo it to me. Because that's the way to get something where you can be assured of the privacy and the control and confidentiality.

**Matthew Todd**
I can see how the strategy that you talked about in terms of not just having the app, but then opening it up via API's, and everything else reinforces that vision.

**Sarah Norford-Jones**
I think it also for us, as long as it's out there and it's being used, it doesn't matter in what form that is, which is why we decided to have a white label side of what we're doing. Also, we're happy for businesses to take certain parts of the technology that we have, and we offer and integrate it. We have a vision for Yeo to be the secured inbox but we're, we don't mind how it looks now. We don't mind if people want to take our technology and call it something else, or integrate it into what they already have. Or, powered by Yeo.

**Matthew Todd**
Yeah, your eyes only is very much category defining in terms of a way of communicating and sending data, as you say, it's the secure inbox, it's controlling, making sure that the person that you intended to say it is actually the person that is, is seeing i. I think that's as much about the positioning of your platform, the capabilities. And the problem, as it is with the underlying technology as well. It seems like those two things coming together, it could be extremely powerful and changing those communication styles.

**Alan Jones**
Integration is the key. Trying to change human behavior and the way, the way we use these tools that we use every single day in our business life is, is incredibly difficult. So if you're able to seamlessly plug in, so it becomes another feature rather than another application to learn. I believe that it would make the adoption of of the Yeo secure platform much easier.

**Alan Jones**
We hope to win from a regulated industry and the business and product point of view against companies like Signal, we will have a tremendous consumer application, very secure with the most amazing privacy rights, etc. But because of that, they're unable to provide a backup. So they can never ever provide an audit path, which is required by regulated industry. So you've got Yeo with similar encryption capabilities, a similar privacy policy, but with the ability to have a third party depository as an audit trail. But even then, that requires the facial recognition. So you get the ultra security, but you do get the ability to address regulated industry as well.

**Matthew Todd**

So you're kind of combining those two elements, you're not having such a big trade off, but you are building for those specific, regulated use cases. But still very much with that security and privacy at the forefront.

**Alan Jones**
Yeah, absolutely. It's a difficult one to manage. But I believe that we've now come up with a way of doing it in order to satisfy compliance officers, etc, within these businesses and to maintain the integrity of the communication.

**Matthew Todd**
That sounds like quite an achievement that sounds like that could genuinely be be game changing in terms of the way way people communicate. For any other founders of a tech company listening to this conversation, based on your experience of getting yo to this point, what advice would you like to leave them with from this episode?

**Alan Jones**
I would say first of all, go in and get some training before you start. It's almost like it's a marathon. It isn't a sprint. So be prepared for it. Make sure that you have the staying power. Never lose sight of your goals. Be prepared to tank along the journey. Something else that I always tell young founders and friends is basically be as a startup as an entrepreneur and as a startup, have an ultimate goal. But be prepared to address it in the same way you would channel crossing in a yhact. So you need to allow for the wind and the waters and many other things that are going to throw you in one way or another, many outside of your control. Keep your eye on the horizon. Keep your eye on your goal and you'll get there and select your partners very carefully. I'm very lucky. I've got somebody that is not only close to me, but well, very tenacious, intelligent and capable and can tell me straight when they believe I'm wrong. I think as, as a founder, listen, take on board, you might not like what people say. But take it on board, process it and come back out and be better.

**Matthew Todd**
Thank you. I think that's great advice. How about you, Sarah?

**Sarah Norford-Jones**
One thing that Alan always says, which is something that I've always kept hold of is, don't fall in love with your product, because love is blind. So be passionate about what you're doing and be passionate about what you're trying to achieve and your goals. But don't fall in love. If we were completely in love and blinded by what we were doing, we wouldn't have been able to change and shift and adapt it to what the market wants. So I think that's always a good one to leave pupil with.

**Matthew Todd**
Yeah, absolutely. certainly see a lot of people. Yeah, falling in love with their solution. A bit too much, often, more than the problem that they're actually trying to solve.

**Alan Jones**
That's the that's the other nuggets, isn't it? Address problems. Provide painkillers, not vitamins.

**Matthew Todd**
Yeah, absolutely. Couldn't agree more. But yeah, thank you for both for a really, really interesting, insightful conversation. As I said a minute ago, I think any founder or aspiring founder will want to be able to take a lot from this conversation. So thank you for sharing the journey so far. I certainly look forward to keeping track of Yeo seeing a developer and I really, genuinely wish that a lot more companies would use your platform like it to take our privacy security a lot more seriously. So thank you for the time much appreciated.

**Sarah Norford-Jones**
Thank you for having us. Yeah, great to speak with you.

**Alan Jones**
Thank you very much.

**Matthew Todd**
Thank you for joining me on this episode of Inside the ScaleUp. Remember for the show notes and in depth resources from today's guest. You can find these on the website insidethescaleup.com. You can also leave feedback on today's episode, as well as suggest guests and companies you'd like to hear from. Thank you for listening.