EPISODE 1314

[INTRODUCTION]

[00:00:00] JM: Ryan, welcome to the show.

[00:00:02] RN: Yeah. Thanks. Great to have me. Or great to be here.

[00:00:05] JM: Great to have myself in the podcast. Leave that in. Leave that in. Leave that in.

[00:00:10] RN: Oh my God! It's Monday, man. It's the first day of Q2 or Q3, and it's Monday.

[00:00:15] JM: People like authenticity. What kind of coffee are you drinking? It's 1pm. Why are you drinking coffee at 1pm?

[00:00:21] RN: Because I need it for the aforementioned reason of Monday. But, no. It's from the empanada place down the street in Redwood City. So the coffee is shockingly okay. But it's like when this place advertises itself as a cafe, but then the milk is just a big bucket of the like minimu packets that you're like, "Okay, maybe this isn't actually a café. Maybe it's more of an empanada place and not an empanada café."

[00:00:45] JM: Probably they have great empanadas, though?

[00:00:47] RN: They do. I've got my second one from lunch right here. And it's calling to me.

[00:00:52] JM: And you're sitting in an actual office right now.

[00:00:55] RN: I am. It's been fantastic to actually get out of my house for a few minutes.

[00:01:00] JM: Really?

[00:01:00] RN: Yeah.

[00:01:01] JM: And how many people work at Material Security these days?

[00:01:04] RN: 20 something? 25, 6. I don't know.

[00:01:07] JM: How do they feel about the office?

[00:01:10] RN: We have always been pretty remote friendly. Like early on, we hired a bunch of folks at Dropbox. And like most of the Dropboxers were into piecing out of the Bay Area before it became mainstream. And then during COVID, we didn't even like look where people live. So the office is largely kind of like if you want to get out of the house and like hang out with people. It's not like a place that ever really required doing work. I think we got to series A without ever having an office and just kind of working out of random people's apartments and Esther's German Bakery and Los Altos. So yeah, office has always been optional. I think when you start the company and you rely in the office, it becomes part of like how you distribute work and like how your governance system and accountability and whatever works. But like when you don't have that, your company from the ground up is a little more resilient. You don't have to like hunch over the interns and make them do work and whip them and stuff. You can just, I don't know, talk about it.

[00:02:02] JM: Is Esther's German Bakery in Los Altos particularly good or just particularly amenable?

[00:02:06] RN: Esther's German Bakery is fantastic. One, you can just sit in there all day and they have unlimited coffee. We tip them really well because we drink a lot of coffee. Two, like any place that gets like German pretzels in the Bay Area is sourcing it from Esther's. And so it's just fantastic. And they have something for every time of day. It's in Los Altos.

[00:02:24] JM: I'm not seeing it. Esther Sherman bakery.

[00:02:27] RN: No. No. Esther, like a person, a woman's name, Esther. She has a German bakery.

[00:02:34] JM: Oh, Esther's German Bakery.

[00:02:36] RN: Right.

[00:02:36] JM: Esther German Bakery.

[00:02:38] RN: Yeah. So at breakfast, they'll have the biggest, heartiest meal you need as a startup founder. You can get like a gigantic stack of pancakes or big German waffle things, and it's great. And then at lunch you can get a very tasteful little sandwich if you need it. And then for dinner, you can celebrate whatever milestone you had as a startup with a gigantic half liter of delicious German beer on tap, and pretzels, and have a beer garden on the back porch. It's the first place I met my series A, B, C actually was it was in that beer garden. So yeah.

[00:03:12] JM: Trivia night every Tuesday. They have trivia night.

[00:03:17] RN: Yep. I thought this was software podcast, but it's actually just – It's an influencer marketing for Esther's German Bakery.

[00:03:24] JM: Live music and sing along second Thursday of every month at 6:30pm. So after COVID, I'm totally down for a live music and sing along.

[00:03:34] RN: There's a back porch. I think it's pretty COVID friendly as long as you keep your distance.

[00:03:38] JM: Second Thursday of every month. You can do that in Google Calendar. I'm going to do that. So how about this email security? Most of the security companies I've talked to, I feel like mostly do stuff on the server-side, and you have some kind of AWS plugin or a GitHub plug in. If you're trying to secure the inbox, is that considerably harder? Do you have to install an agent on my browser to monitor my Gmail? How do you do email security these days?

[00:04:08] RN: Sure. Yeah, I mean, security is all over the place. It touches – It's applied systems. So there's every kind of security that exists like name a kind of technology, there's a kind of security industry for it. When it comes to email, traditionally, people think about it as like a firewall. Emails are coming in, and you're going to send them to some other service that's going to look at the emails and vet them and scan them before they arrive in your mailbox. That's how – If I send you virus.exe to your Gmail from some sketchy thing, like it's not actually going to get delivered, right? Google will block stuff. And Microsoft's the same way.

There's a whole kind of cottage industry going back like 30 years in email for things like spam blocking, right? And so you can see like trying to check that link to see if it's something that wants me to type my password in or check that attachment to see if it's something really tricky. It's primarily like a bouncer in front of a bar, that security model, right? And then simultaneously, if I own a big company and I'm worried about people sending stuff out going an email that they shouldn't, then you'll put something in the wire that also checks emails on the way out. So email is historically kind of like protected, like the form of network security, right? Like networks, it’s all about firewalls. Like you can't connect to Port 22 because I said so, right? Or you can if I like where you're coming from. Just kind of gateways, right?

And so that's kind of what led us to making this company, because the thing that inspired me a long time ago in 2016 when I started working in this space was the John Podesta hack, which happened on a personal Gmail account. And so the number of times that comes up, it's like pretty high, and you don't get to control the network on personal accounts, right? Email goes to @gmail.com. You actually look at the NS records on gmail.com and it says MX goes to this server, and you don't get to change that. So the whole existing email security industry couldn't really do anything because of that, right? So like personal accounts were just not a thing in the security industry, because the whole security industry is used to selling email security to businesses that control their domain, right?

Obviously, like nowadays, people are using Office 365 and G Suite or Google workspace or whatever for their work, but they still control their domain. The first thing you do is you change DNS to point to Gmail, but you could have it point to any of the existing email security vendors and then have those things routed to Gmail. So the point is we protect email way different than most people do, because the kind of problem that brought us into this space was not something that any of the old things could do. And so as a result, the techniques that we invented for protecting personal accounts ended up being really, really, really cool and we brought them into corporate environments, because necessity is the mother of invention. Does that kind of make sense? So you can't do the traditional thing. So you have to be creative. And then if you're creative, oh my God, there're a lot of problems with email at work too.

[00:07:18] JM: The canonical problem that I think about is I somehow get an email with a PDF in it. It makes it through my spam filter, and then I download the PDF, and it does some malware related stuff. How close to the average email security problem is that?

[00:07:39] RN: Yeah. I mean, it’s as traditionally conceived by like everybody that buys and sells security software, like that is something – Like the fact that something malicious was in that that didn't get caught or whatever, whatever is like a gap in your existing solution. And there's someone trying to sell you like a newer firewall or something that will try and scan everything. But the problem is, is I can send you stuff that will get through any like gateway, right? For example, I can send you something at scale to your company that has malware, but it's inside a password protected ZIP file that's actually encrypted, right? And then I could trick you into typing in the password and then detonating it.

So when we talk about email security, like there're just a lot of problems with the traditional like someone checking all the emails before they come in, because you could always get something through the TSA checkpoint. You can always get something through any doorman, or firewall, or gateway, because the point of emails is to send someone an email. So we care about email, basically all of these problems that nobody previously ever really cared about. Everyone's so focused on like blocking the obvious stuff that like the what happens if I get in your email? Like what happens if I hack some app that you OAuth’d and then now I have email access and I didn't send you malware, right? I’m in your email.

So in other words, I could talk at length about the problems that exist in email totally independent of like, “I can send you tricky files.” But like the point is everybody else in the whole space is like thinking about things like a firewall, and it kind of like blows my mind that people aren't a little more creative when you think about this stuff, because we all use it every day.

[00:09:19] JM: Okay. But email, I think, Gmail. I use Gmail in the browser. To me, that is the best, the purest email client these days. I don't really want to use Superhuman. I haven't tried it yet. I kind of want to try it, but I just feel like with Gmail, you're closer to the metal. In terms of actual email clients, I like Gmail, I like streak. Do you need to get into my Gmail? Like do you need to have a Gmail plugin or something?

[00:09:47] RN: No. No. No. Our whole our whole app is just an API client. Like we talk to Gmail. When we're protecting a personal account in Gmail or a corporate G Suite workspace thing, we just use the regular Gmail API. We're not a client or a plugin or anything. No. I mean, we sell to companies with like hundreds of thousands of people. Like if we had to install like a client or a plugin, like we'd be in trouble. So it has to work across clients. Like our stuff works with Superhuman. It works with the regular Gmail client. We're just an API consumer.

[00:10:17] JM: Your company's counter intuitive in a lot of ways. And that's because, I think, when people think of email security, again, they really just have this hard variable assignment in their brain where they think email security means scanning for PDFs. And I feel like you're taking it a lot deeper. And I really want to just emphasize that. So maybe you could explore – Can you just give me some like very simple, but like shocking facts about email that will convince people that email security is like a really, really broad domain?

[00:10:49] RN: Okay, yeah. So for example, I don't know if you followed what happened with this HAFNIUM APT this year. So the Chinese government controls this thing called HAFNIUM and they found some zero days in exchange, all right? They found four of them, in fact, and they used all four of them so that any like exchange server on the Internet, they could just go and download all the contents of, right?

And so what's different about this one versus prior ones is that they didn't just do it to go after like a couple companies and like whatever Tibetan activists that they usually go after. When they realize that they were like getting found out, they hit like 100,000 different organizations, and they downloaded the email of 100,000 different organizations. That's a problem that we care about, for example. You can go on our site and our love page and like see people talking about this HAFNIUM thing. Or with the case of Solar Winds, right? Like they actually went and compromised this vendor, Solar Winds, the Russians, and/or depends who you ask obviously. So then after they did that, they did this whole elaborate thing just to hack Microsoft itself. And then once they got into Microsoft, then they started raiding people's Office 365 so that they could steal email.

So email is two things, right? In security, there's two concepts, right? There's something called a vector, which is how I get you. And there's something called a target, which is what I want, all right? And when you talk about email like I'm going to send you some tricky thing that maybe you'll click on, we're just talking about email as a vector that maybe I got you to click on something, but then I got your laptop after you clicked on that. And now that I've got your laptop, what else am I going to do? And blah, blah, blah, blah, blah, blah, blah, right?

But like email is also a target that people actually want to the point that they'll burn four 0 days to steal it, right? Or they'll go and compromise like elaborate software suppliers to be able to get it, right? Or you know what? Even if I compromised your laptop, the first time I'm probably going to do inside of corporate environment is open up the email client and download everything that's in there, because everybody is talking about everything and doing everything and whatever. Like I'll compromise your laptop, I'll open up your email client. I'll see you talking to somebody else about a payment. And then I will slide into that thread and then change the account number and say, “Oh, no, could you send it here instead?” And then I'll steal like a million dollars from you on a wire, right?

So the point is people are trying to get into your email. And then they're not just trying to send you tricky things, right? They're not just trying to send you malware. If I get into your email, for example, how many things do you sign into with your email where your emails like your username and stuff? Like most things, I assume, right?

[00:13:36] JM: Or more specifically, my Google account.

[00:13:38] RN: Yeah, but it's still like –

[00:13:41] JM: There's a bit of a distinction, but it's the same thing pretty much.

[00:13:43] RN: Right. What happens when you forget your password on most apps?

[00:13:46] JM: Yeah, everything goes through email.

[00:13:48] RN: Right. So if I get into your email, I spread to everything else, and I can get everything else too, right?

[00:13:53] JM: It's the single point of failure subject to two-factor authentication basically, which is horribly weak, which is horribly weak. Two-factor authentication is like super weak, super defenseless, like. Can be routed through an insecure SMS infrastructure. Effectively not secure at all.

[00:14:14] RN: I mean, it depends on the actual second factor, of course. Like if you're using Webauthn or YubiKeys or something, like you're in far better shape than if you’re using SMS two-factor.

[00:14:25] JM: But I think there's vectors where if you push on it further, eventually it routes to SMS infrastructure, which is, yeah, people –

[00:14:32] RN: People fall back on SMS, which, yeah, it blows my mind. Like I don't know why they do that. But a modern MacBook actually has a Webauthn token built-in touch ID. You can use face ID now even as a second factor.

[00:14:45] JM: By the way, I become an Apple person because of security. I've just become an Apple person.

[00:14:50] RN: That’s their brand man. That's what they’re going after.

[00:14:52] JM: I finally see it. It's pretty amazing. Once you finally see it, once you finally see how important this feature is, you can't really go with Android. As good as good as Android software is, as bad as Siri is, and as much as I want the Google assistant, you actually just have to bow down to the gods of security.

[00:15:10] RN: I mean, I think Android is an ecosystem. Obviously, some like LG phone that hasn't seen a patch in two years is not going to be in great shape. But like the people that are doing device security on the pixel phones, like they know what they're doing. Are they as good as Apple? I don't know. But, I mean, –

[00:15:25] JM: Alright. Hey, look. Let’s get a little controversial here. So, proposition, iOS is more secure than Android partly because it is closed source proprietary software. True or false?

[00:15:41] RN: I mean, well, one, like the whole thing isn't closed source. Like Darwin and stuff is –

[00:15:47] JM: No evasion. No evasion here. Let's go straight to the heart of the matter.

[00:15:50] RN: You might as well be saying like Vim versus Emacs here, right? Like saying is open source software more secure or less secure is like it's a complicated thing. Have you read like Cathedral in the Bazaar? What is it? All bugs are – What is it? With enough eyeballs, all bugs are tractable, or all bugs are simple or something, right?

[00:16:06] JM: It’s true. But that's an eventually consistent system.

[00:16:10] RN: Apple, to be clear, is a substantially bigger target. There's a reason like NSO group and stuff prioritizes iOS malware over anything else, because like every CEO and every executive is using an iPhone because they're fancier and prettier and nicer. So I think there's – What's really funny is you're asking fundamental questions about – I guess if you want to say open source versus closed source, what's more secure? Like that's the specific lightning rod that you're asking and holding up into a thunderstorm right now. We can discuss that. But in general, the centralization versus decentralization is the more interesting thing, because a lot of times you see it in security. People are like, “Well, if I put all my eggs into one basket, it will be easier to secure and monitor the basket to keep the basket patched and whatever, whatever,” right? But then they're like, “Oh my God, I put all my eggs in one basket. And now you can lose all the eggs at once in the one basket,” right? And so security is complicated. Anybody who's listening that that thinks security is easy, or is curious about security and doesn't know why all these idiots keep doing dumb things, like –

[00:17:07] JM: Okay. Can you stop the evasion now? Come on, man. We need to talk about ransomware eventually, and you're evading right now on the smartphone question.

[00:17:15] RN: I would say, empirically, iOS has been more secure than Android, because Android is not one thing. It's an ecosystem. It's like saying is Windows more or less secure than iOS? Like anybody can make a Windows machine? Anybody can do –

[00:17:29] JM: Well, no, we know the answer to that question.

[00:17:31] RN: Well, sure. But I don't think that there's one answer. And even the way of saying that, well, this thing is more secure than that thing. And thus, you should do this. Make your own choices.

[00:17:41] JM: It's kind of true. Here's the other thing. When I think about the actual bugs in iOS that have appeared over the last, call it 7, 8, 9 years, whenever there's a really savage like ownage of the iOS platform, it's just relentlessly savage. It just destroys people so badly. It's like the platform is so generally impenetrable, that once it gets penetrated, it just can wreak complete havoc.

I feel like there have been some security flaws in the iOS platform over the years that have been like really, really shocking and horrifying. Am I mistaken? Or it feels like they're like more severe than on Android?

[00:18:18] RN: I think a lot of this is a function of how they're reported on, because like all the people that you want to hack, if you’re the bad guys, are using iPhones.

[00:18:26] JM: They're using iPhones, right? True.

[00:18:27] RN: Yeah. And the like casual, like I'm going to have some sketchy app in the app store that is like you think is a weather app, but it's actually selling all of your app data to some black market GDPR non-compliant reseller who's eventually selling it to App Annie or something, like there's sort of low-level suckage is the nature of the beast in Android? Whereas, yeah, iOS, like, “Yep, it turns out that the Saudis bought a thing from the Israelis that let them go and read the iPhone of all the people that they want to hit with the bone saw or whatever.” Like it has to be little more dramatic and targeted in iOS land. I'm with you there.

[00:19:02] JM: Whenever I take a moment to look at the soft underbelly of the Internet as viewed by security vulnerabilities, it just makes me really sick. Like I just get a little bit nauseous. Whenever I look at ransomware stuff, whenever I look into ransomware, I just get a little bit sick, or cryptojacking. All these, it just creeps me out, man. Modern security is so creepy. Don't you feel that way? Don’t you ever feel that way? You're just like, “Holy crap. This stuff is kind of dangerous.”

[00:19:28] RN: In my mind, there's this race, okay? There's a race. And it's going basically between what are the new things that technology can do for me versus like what is that exposing me to? Because security, it's a time delta, right? It's, “Well, you invented this thing.” And then, “Oh my God! The unintended consequences of the invention of this thing,” right? And the nature of technology when you zoom out, I know you're an enthusiast and philosopher on the nature of this stuff. Computers are always doing more for you than they were doing last week. All right? So it's an expanding – It's a balloon or it's an expanding circle. It's like ripples in a pond as technology does more and more and more. And then the reason security is a huge pain in the ass is because it's trying to play catch up with something that has an expanding surface area, right?

If the only computer I used was an ATM to get cash, which I then walked over to the farmers market or something. And we're talking about like the 80s where that was like the only computer the average person used, then like you only have to protect one thing. But like, seriously, your whole damn life is accessible in your phone now. And so it's doing more for you. That means like people like me are the cleanup crew for the rest of the technology industry for the rest of society as it becomes more and more computerized. So like the reason it's scary for you is because of how much of your life is now tied up in this stuff, right?

[00:20:49] JM: Well, and this is – Let's change the subject. Honestly, I can't talk about – Seriously, I just don't even want to talk about this stuff. It's just like it's too – It's a little bit too creepy for me to even talk about on air. It's like too blackmarish marriage, because I think about it – Do you know what I'm talking about here? Like do you know like the kind of things that I kind of don't want to talk about that just make me sick? Like when you're in a position where you can imagine things in security and they really, really creep you out?

[00:21:14] RN: It's such a security, man. It's like the unintended consequences of how much technological change has happened in the last 20 years. We are going to be feeling for a lot longer than 20 years. So one of my favorite sayings is technology spreads, because it's useful, not because it's safe, right? So it will cover the entire human experience. It will cover the whole globe, right? You will use it 100 times a day before the implications and the unintended consequences of that are anywhere apparent. And security is just one of many things. So it would make you very disquieted. I know for a technology person, I'm kind of a Luddite, but it's really important.

[00:21:52] JM: I started building a few companies recently, a few other companies other than Software Daily. Because with Software Daily, we have a really good CEO in place. So I've been moving on starting these other companies. And I started a payments company and a gaming company. We've raised money for both of them. And one of the employment exercises that is true at all of my companies is you have to learn to play poker. So basically, all employees at each company that I work at that I'm a shareholder in need to learn to play poker. And the reason for that is you need to know how deeply exploitative other people can be. Like you just need to know that. In today's world, with all the attack vectors that we have, you just need to know – Like you need to understand depravity at scale is my perspective.

[00:22:40] RN: Is this one of Joseph Conrad approach to being a software CEO?

[00:22:44] JM: It kind of is. It kind of is. I just feel like that's the world where we're headed. It's a little bleak, to be honest. I don't know. Do you feel the same way? Or do you feel optimistic?

[00:22:55] RN: This obviously gets pretty obscure, but I read as much history as I do sci fi, and like there's a lot about the human condition that's like pretty damn bleak in prior years. And so I would say that the classic like Orwellian consequences of the technology that we have now, it's obviously there. But there's a lot to like about the future. It's going to take like smart people doing their best to like believe in the values of individual freedom and privacy and stuff like that. Like it's a fight that will never be won, but I think it won't be lost either, right? So there's no reason that the future has to be Orwellian or bleak. And there's a lot to like about how cheap communication is and how accessible information is, right? Like there's a lot of ignorance in like the world of 100 years ago that would be like completely like mysterious and like impossible nowadays, right? Like people died for the lack of knowledge about basic things, right? So I don't know. I think that the world is definitely getting better. I mean, it's a kind of like are you a Steven Pinker, like better angels kind of person or not? I think I am. But it means that you're always going to have to keep it together. And you're always going to have to be fighting for whatever values you believe in. My personal ones are obviously like liberal democracy, individual freedom and things like that, right? But privacy is quite important. And it constantly needs to be re-litigated and re-articulated in every generation. So I don't think technology makes the world into shit. I think it makes the world different. And good people have to fix the world constantly. Every generation needs to fix the world because of something technology did to it. Imagine two generations ago when we were fighting over atom bombs. Like, "Yeah. Oh my God! My iPhone can get hacked. That would be so bad for my life." Yes. But like we now had the ability to nuke the entire planet and turn it into glass. Like technology give it and technology take it away, and every generation has its fight. And so I'm trying to do my part in this generation's fight, but I'm not hopeless. I'm never hopeless.

[00:24:59] JM: All right. Well, I'm presenting the fork in the road. We can go more obscure, or we can like randomly move into talking about engineering management and email security company.

[00:25:09] RN: Whatever you want, man. Sure.

[00:25:11] JM: Okay. Let's go obscure. Let's go obscure. Proposition, we're already in the metaverse. Zoom is critical to the metaverse. Clubhouse-like experiences are critical to the metaverse. Shared group messaging is critical to the metaverse. Group VoIP calls are critical to the metaverse. Air Pods are critical to the metaverse. Low-cost Bluetooth headsets are critical to the metaverse. Do you agree that we are in the metaverse?

[00:25:44] RN: Yeah. I mean, obviously, it depends on exactly – I think you're bringing this up because like Zach used the term metaverse a bunch recently to describe his ambitions or something. I largely avoided that because it looked confusing. But like I always think about like there's a – I think I read a lot of like post-modernism at a very like vulnerable time in my life when I was a teenager. And I kind of think about like – Even this interaction we're having right now on Zoom. Yes, it's remote, whatever. But like it's piggybacking on all of this like machinery that we have psychologically based on like when our ancestors met in the forest and needed to determine like friend or foe or something. It's this very natural thing, but it's also very artificial at the same time, right? It is keeping the legitimacy of a face-to-face meeting between human beings. And instead, it's abstracting. And each of us could have weird Zoom filters on. You wouldn't even know what I look like or who I am, right? Like we're assuming that the image on the screen is truthful and that this is my actual voice and all this stuff.

So I don't know. Like all this stuff became abstracted a long time ago. When people started doing fantastic works of art in a way that's like distributed across thousands of people online. When we realized like the power of like wikis and Wikipedia. Like I think the Internet was a metaverse and it's just been growing and growing and growing to the point that like real life and physical life. I think COVID is sort of where it jumps the shark, right? And you're like, “My life is in the computer.” But every once in a while I meet these weird meat sacks in person, but I might get sick from breathing their air. So I think it's been sneaking up on us. Most things involving technology tend to sneak up on you. So I think the metal versus this coming up on 30 years old personally. But I think it started with like the printing press, and it's just been getting weirder since then.

[00:27:34] JM: Can I tell you something that depresses me an infrastructure these days?

[00:27:37] RN: Sure.

[00:27:38] JM: Everybody has taken their eye off the most important ball. The most important ball is zero cost transactions and micro payments. And the only people that are working on that are like the layer two cryptocurrency people, and they all seem politically wrapped around the axle. So they're not actually going to get this thing done. Like lightning network has been around for what? Three, four years, and yet we still have expensive payment systems. Like all of this stuff is moving at such a slow pace. And in the meantime, we have the best companies in the world that have high-margin cash cows. And basically all they're focused on his like moderation and metaverse BS, and like virtual reality this, and mobile that, and ad tech this, and search engine stuff that. It's like, “What are you guys doing? Where's my zero cost micropayment system? Why can't I send five cents to a Nigerian knowledge worker? Like why can't I do that yet? Why can I send an email to anybody? I can send a Slack message to lots of friends, and I can't send 12 cents or like three satoshis to somebody? What's going on? Why can't anybody build this stupid thing?” It's really aggravating to me. Do you ever get aggravated about stuff like that? Like stuff that you don't really feel like you have a control over?

[00:29:04] RN: I definitely had to do some thinking on like the real – I'm not a big cryptocurrency person. I'm more of like a social commentary, like thinking about systems. I don't have a dog in the crypto race or anything. But like I think what it exposes is just how like political the monetary system truly is. It's a tool of social policy. It's a tool of foreign relations. So like all these governments, actually, at the end of the day, kind of like their currencies. And like just because you want to have like a decentralized PayPal or some Patreon with no minimums. And like the idea of like money is just information. And if information is basically free, why isn't money free? Well, it turns out there are some key differences between money and information. And like it took rock bottom. It's took Facebook being like, “Well, we could do this.” And then every government in the world being like, “Oh, no, you don't.” Because like there are political forces in the world that undergird and supplement and occasionally are in direct competition with the technological and economic forces in the world. And it turns out money is politics too.

So the reason that none of the top tier companies are fighting for this zero cost five cent payments to Nigeria or whatever is because the ones that do get smacked down by governments. Facebook tried, and it got smacked down. The only thing worse than publicly administered money is privately administered money?

[00:30:31] JM: You're kind of dissing Facebook Libra there, right? Like you're basically saying that like the only thing worse than government administered money is privately corporately administered money, right? That was what you said.

[00:30:43] RN: Sure.

[00:30:45] JM: Facebook Libra, first of all, I'm not going to dispute you that it's probably not the best semi-decentralized payment system. But it's a semi-decentralized payment system. That's what it is. It's not a private payment system. I mean –

[00:31:03] RN: Sure, sure. There's no single point of truth, whatever. But it's still a network and the network still has influence.

[00:31:10] JM: Okay. So Libra, Libra was hilarious for many reasons. And it was obvious. The sad thing about Libra, what really made me sad, especially as somebody who like is a huge fan of Facebook. I mean, I literally spent two and a half years writing a book about the company. It's a referendum on how people see Facebook. If you look at this case study, it's basically a referendum on how poorly Facebook is regarded by the general business community. Because what happened is they did this consortium thing. Do you remember this? Like they did this, the consortium of –

[00:31:43] RN: It was like Visa and all these other companies.

[00:31:46] JM: It like the most random coterie of high-profile companies. It's like very random coterie. It was Andreessen Horowitz, who – You're an Andreessen Horowitz portfolio company, right?

[00:31:57] RN: Yeah.

[00:31:58] JM: It's like Andreessen Horowitz, Stripe, PayPal, Visa, like whatever. It's like the cabal, right? It was a cabal clearly, like Goldman Sachs or something. Just like cabal of people who are going to oversee the financial system. Actually, it's a great idea. But the messaging is so like blatantly like, "Hey, we're Facebook. We're just we're just allocating power. Do you guys have a problem with this? What's the big deal?" And then it's like, obviously, like the messaging is just like, "Seriously?" And so everybody just immediately is like, "Okay, this is the stupidest thing ever. Why would we put the monetary system in control of the Facebook-ordained cabal of financial arbitration? What? We're doing that?" And then so Stripe pulled out, right? Didn't Strike pull out within weeks of this announcement? And it was like –

[00:32:54] RN: Yeah. Rush to the exit is pretty fast.

[00:32:57] JM: It was like, "Okay, so the best company in the world pulls out of the Facebook-ordained financial system." Or was that just like Stripe's like straight up dagger into Facebook?

[00:33:09] RN: No. I mean, what the cryptocurrency people don't seem to understand – I think it dawned on me one day that like all the things you know as a software engineer about like open source project governance and like all the soft power of who decides, like the community, but what forks get merged? And is it Linus and Guido van Rossum versus the open source, whatever, whatever? Like everything you know about the politics of an open source project globally and how it's used and how it's developed and what the roadmap is, like the underlying cryptocurrencies themselves might be decentralized, right? It's not like one bank controls the master ledger of anything, but what they do is it takes everything about open source project governance. And it kind of treats it like the Federal Reserve, right? So like there's a ton of soft power in being like the Linus Torvalds of Ethereum, right? Obviously, the Vitalik guy or whatever does that. But my point is just because something –

[00:34:04] JM: The Vitalik guy?

[00:34:06] RN: I'm not a cryptocurrency person.

[00:34:07] JM: Vitalik Buterin?

[00:34:09] RN: I don't know these people. I just watch the system.

[00:34:11] JM: The Vitalik guy.

[00:34:13] RN: I didn't claim to be an expert .You brought this topic. My point is like just because something is decentralized does not mean you want whoever controls it to control it. In that case, Facebook is literally the Federal Reserve Libra or whatever. And I like the Federal Reserve, because it's created by Congress and which is a representative thing that I can influence and vote for and stuff. So like my monetary system I like wrapped up with my political system. And just because something's on the Internet, and just because something doesn't literally have a master ledger, does not mean it's free or just.

[00:34:44] JM: Okay. No. No. No. Hold on. Hold on. Hold on. Hold on. Hold on. Hold on. Okay, you don't want one financial system, man. Like you want a multitude of financial systems. Like this whole – Dude, how many –

[00:34:56] RN: I'm an American. I like one.

[00:34:57] JM: How many operating systems do you have in your life?

[00:34:59] RN: I mean, a couple. But besides having the word system in them, why is that relevant?

[00:35:04] JM: No. No. Bear with me. How many operating systems you have in your life?

[00:35:09] RN: So there's Android, Linux. Linux, Darwin, BSD, whatever. And like, whatever, Windows, like 64bit kernel. So it depends how you draw an operating system.

[00:35:20] JM: How many different Linux distributions are involved in your life?

[00:35:24] RN: Everything runs Linux. How many Amazon devices do I own that are currently running some random Linux kernel? So yes, dozens.

[00:35:30] JM: Okay. And what is the cardinality of random Linux kernels that are running those various systems?

[00:35:37] RN: They're probably all on different kernels. Is in kernel versions? Like how many Linux kernel versions –

[00:35:43] JM: Well, I would actually take like unique product fingerprint of operating system cross hardware that it's running on. So that would be my like unique fingerprint. Anyway, where I'm driving with this is you have a multitude of operating systems, and then hardware sets, and firmware sets and whatever sets that you run on in your life. So like the same is going to happen with payments, right? You're going to have a multitude of payment systems, right? That's this company that we're starting called Rectangle. It's basically Linux for payments. By the way, the round is not closed yet. We're still trying to wrap up this round. It's ridiculous how long this is taking. But we're doing Linux for payments, because you want like different embedded payment systems, right? You want a multitude of embedded payment systems.

[00:36:28] RN: Do you mean the actual like underlying currency ledger? Or do you mean like last mile clients software, or what?

[00:36:36] JM: You basically need a Zapier. You need to open source Zapier for money. So take the simple use case. I swipe a credit card. Or no, more realistically, more realistically. I'm a merchant. I want to accept Fiat. My customer has crypto, okay? So like you come to my open source decentralized Shopify clone where I sell hats. I'm a normal guy, right? I just sell normal hats. They just say Software Engineering Daily on them. You're a crazy weird security enthusiast who likes crypto. You only have crypto. You need to pay with crypto. I want to accept Fiat. The middleware there is a Rectangle, a Rectangle kite. It's like basically like a Zapier zap kind of thing. We have kites. So like the conversion module. We produce conversion modules. They're open source. We host them, but they're open source. We also tell you how to host them. But basically there're all these Zapier zaps for money, or conversion modules. That's what we do.

[00:37:39] RN: And then who takes the actual financial transaction risk of converting the currencies?

[00:37:43] JM: We do. We do. And we price that in. So it's like we're not cheap, right? Like we're kind of terrible. We're kind of like a terrible, expensive service. We're like Stripe, but more expensive, basically.

[00:37:57] RN: It's a good one. Cool. Yeah. I mean –

[00:37:59] JM: We're like Square, but we're a rectangle.

[00:38:02] RN: I got it. Like a slightly more less constrained square, rhombus even. Some form of quadrilateral, parallelograms and trapezoids are also involved.

[00:38:11] JM: So we're the founding member of the Quadrangle Consortium, which is a division of the Shapes Consortium.

[00:38:18] RN: Is this becoming like object-oriented programming lesson at some point?

[00:38:22] JM: No. It's more like a shapes-oriented proclamation.

[00:38:27] RN: I see. I'm down. Yeah. I don't know. It's just, I'm an American, and I like dollars, because dollars are how the US projects power.

[00:38:36] JM: I get it. But this is my point, though. You want domain-specific payment systems, right?

[00:38:43] RN: Sure.
[00:38:45] JM: Do you use gRPC for everything? Like I use WebRTC sometimes. I use gRPC sometimes.

[00:38:52] RN: Last time I checked gRPC, it doesn't work in browsers.

[00:38:57] JM: You can do like protobufs over browsers, right? Like you can send protobuf –

[00:39:00] RN: You can send me an Ajax request with a protobuf in it, but gRPC itself doesn't work. Like you can't write a native gRPC client on the other end of an AJAX request.

[00:39:09] JM: But theoretically, something like that should work, right? You should be able to do gRPC over WebSocket or something, right?

[00:39:16] RN: GRPC, it's actually not – You're using the term I think a little bit differently. You can send protocol buffers, and you can make protocol buffers for function interfaces, right? But gRPC is like a specific like wire level protocol that supports like streaming and blah, blah, blah, blah, blah, blah, blah. Like if I have sockets, I can do whatever I want. But like, yeah, you'd have to – I think you'd have to build it directly on top of a WebSocket and then you'd have to write a gRPC server on the server-side, whatever. But like gRPC itself like should be able to do it, but I think there was like –

[00:39:48] JM: I mean, that's my point. Like if you want to know like next generation, like agro data transfer over WebSocket type interactions, you want to do gRPC over WebSockets. I'm pretty sure. Or something like that.

[00:40:01] RN: Yeah, I mean, it's just a matter of like being clean.

[00:40:02] JM: How do you use WebRTC for like high-fidelity communications protocols? Can you do that?

[00:40:10] RN: Yeah. I mean, this was designed for. RTC stands for like real time communications.

[00:40:14] JM: Yeah. But right now it's only used for like video, right?

[00:40:18] RN: No. No. No. No. No. No. So I've actually done a bunch of WebRTC before. Not as much as my Feras, but like –

[00:40:25] JM: Wait. What's that guy up to these days? I love that guy. I'm such a huge fan of that guy.

[00:40:29] RN: He's still doing file sharing, man. Go and check out his thing. He's got this like wormhole thing.

[00:40:33] JM: I'm a **[inaudible 00:40:35]** fanboy. He's one of these people who is like inspiring as a developer, like Dan Abramoff or – Do you follow Dan Abramoff?

[00:40:45] RN: I bow at the template for Feras. Feras is the only god.

[00:40:48] JM: Okay. All right. Forget it. Alright. That's fine. Anyway, sorry. Continue –

[00:40:51] RN: But my point is you get a data channel. When you do a WebRTC negotiation, like you get a channel that you could send bits along. So you don't have to use it for voice and video. A long time ago, I made like a peer-to-peer like CoderPad, like shared collaborative text editor that didn't have like a backend. That was just peer-to-peer. And I sent all of the like cursor positions, and like what keys you were typing and stuff across the WebRTC channel. So you can do peer-to-peer data over it. Feras actually did a company a long time ago that was like doing a CDN over WebRTC.

[00:41:21] JM: Yeah, he sold it to Yahoo. He sold it to Yahoo.

[00:41:25] RN: And they were loading images over it.

[00:41:27] JM: That guy is so precocious.

[00:41:29] RN: Precocious implies you're young. And we're all old now. So he used to be young, and I used to be young. And now we’re old.

[00:41:34] JM: Wait. Are you his age?

[00:41:36] RN: He's two years younger than me, I think, maybe three.

[00:41:38] JM: That's right. Yeah. I always felt like he was precocious, because I followed him on Quora, because I think he worked at Quora for a little bit. How's go to market?

[00:41:46] RN: I mean, we sell a lot of software these days. It's pretty cool.

[00:41:50] JM: I believe you.

[00:41:51] RN: It's weird having a company that actually –

[00:41:53] JM: Dude, the margins, the margins in security are so good.

[00:41:58] JM: Even the SaaS margins. The margins in SaaS are good.

[00:42:01] JM: But it's cheap to run SaaS, right? Because your runtime. It's not? Am I wrong?

[00:42:07] RN: We process like billions and billions of emails. There's a lot of –

[00:42:09] JM: I'm sorry. Okay, I'm stupid. What's your biggest cost center in infrastructure? Is it Databrix clusters or something?

[00:42:18] RN: I probably can't go like too specifically on how our infrastructure works. But suffice it to say, lots of big data and scanning and processing, lots and lots of emails.

[00:42:26] JM: Big data, scanning, processing, lots of emails.

[00:42:30] RN: What we do is we walk backwards throughout the history of a mailbox, because we're trying to like protect the data inside of it, for example. And so it's not just about like getting turned on and like watching all like new email come in looking for spam or malware. No. No. No. That's just part of it. You have to be able to analyze like 20 years of email, right? So it's a pretty heavy lift infrastructurally to do it. And you have to do it as fast as you can.

[00:42:55] JM: Can you tell me any opinions you have on data infrastructure? Okay, so here's what I like –

[00:43:00] RN: I have lots of opinions on data infrastructure.

[00:43:02] JM: Can I tell you my favorite thing about the Andreessen Horowitz infrastructure investment strategy? The whole portfolio synergy around data infrastructure, where they have like, basically, the smartest data infrastructure people around them. You know what I mean? Like they have DBT. They have Databrix. They have Anyscale. They have what else? Like Census. And so I imagine, if you're doing email security data infrastructure, you can sort of go to the smartest minds in streaming, basically, and really know how to run streaming infrastructure. Am I wrong?

[00:43:36] RN: So I'm like old enough at this point that I've seen like a couple waves of like data infrastructure and stuff. And so I came of age in the valley in like 2009, 2010, 2011 when like the first wave of like Hadoop and Kafka hadn't been invented yet and all these things. And so it's weird for me seeing all of it cycle again. Because like, basically, that wave, it had IPOs. It was great, whatever. But then it basically died. And for a couple years, you couldn't do anything involving analytics in the valley. And it took like kind of reviving big data as like data science, AI, ML something, something, something and it took a bunch of exits like Looker selling to Google and Confluent doing really, really well. Like it took a lot of stuff to get VCs to be interested in general data infrastructure again. So I'm kind of old school enough that I have like my own opinions on like how data should be processed and whatever, whatever, whatever. But Andreessen has done a good job of being well-invested in this wave of stuff. And there're some great companies in there. And then, obviously, like I'm a huge fan of Databrix broadly in general. But I remember when people are like, “This Spark thing, this is a paper. It's got no future,” or something, something, something.

And I think the way that what's really interesting for me is how like the rise of like public cloud by default. And not just public infrastructure, public cloud infrastructure, but the managed services on top of it. Like it used to be like Amazon had Elastic MapReduce, or you could like spin up some Redshift cluster or something. And that was it. Whereas nowadays, the things that come built-in to the public cloud services are so good, that it's been interesting for me watching like the big data ecosystem in this generation be up a couple levels in the stack, or to be really, really focused on certain domains. So just the elaborate dance around the trillion dollar cloud platforms has just been kind of interesting. And that's the most creative thing I think I see an ecosystem is how do you make money when you're not Google, Microsoft or Amazon?

[00:45:39] JM: Well, I mean, on the other hand, you don't have the baggage of being attached to a giant organization.

[00:45:46] RN: Yeah, but they own the actual – And I'm not sure if I should tell this story, but I was talking to someone high up at Amazon. And I remember doing diligence on like Snowflake’s A or B for somebody back in the day. And I was like Amazon's early to this party with Redshift. Like there's no way that like they're going to screw this up. Yeah, Redshift is just par excel. And so it's not going to scale. They're going to need to like redo it. But the idea of having like large scale SQL analytics built into your cloud platform was something they clearly understood, right? And then Snowflake comes out, and they're basically just selling Dremel on top of AWS, right? They're selling BigQuery on AWS and BigQuery on Azure. That's how it works.

[00:46:27] JM: You’re kidding me. Snowflake is based on the Dremel paper?

[00:46:31] RN: I mean, partially. They're like ex-Oracle people too. But like the point is like it is a horizontally scalable large scale SQL analytics warehouse.

[00:46:43] JM: Well, not just horizontally scalable. It's also vertically scalable, because it does like the storage tiering thing.

[00:46:51] RN: Yeah. As in like Dremel is like really tightly coupled to like a bunch of Google-specific abstractions. But like my point is everyone else in the whole world was largely doing like –

[00:47:00] JM: Hey, was it Dremio? Dremio did the Dremel paper also, right?

[00:47:03] RN: No. No. No. Dremio was Tomer’s Company, right?

[00:47:06] JM: Yes. Dremio is Tomer’s company. Apache Drill. That's not Dremel. Sorry. Sorry. Sorry. Sorry.

[00:47:10] RN: Yeah, but it was inspired by it. As in there were a lot of Dremel clones. Like Cloudera made Impala. Hortonworks tried to get there with by like turning – Was it project something, whatever?

[00:47:21] JM: But Snowflake was like a fresh approach, plus experience building Oracle. That's like a magical recipe.

[00:47:29] RN: And they didn't attempt to screw with the Hadoop ecosystem. They just said, “Look, you've got AWS, and you want a really good data warehouse.”

[00:47:36] JM: Okay.

[00:47:37] RN: The whole reason I brought up the story, though, I want to get to the punchline. It's like when I asked the people AWS about this, and like, “How does snowflake – How is it so viable? Like why didn't you guys just have a viable like BigQuery in AWS?” Because they spent a bunch of time like messing with Presto, and Athena, and stuff like that. It sucks. Like I used to run Presto at Dropbox. Like I'm sorry, it kind of sucks. And like they're saying, “Well, you understand? Even if like Snowflake doesn't have any servers, like we get paid when people buy Snowflake,” right? If snowflake sells a bunch of stuff, like we get paid either way.

So what Google, Amazon and Microsoft have is the actual physical machines on which all this stuff is hosted. So like the point is they get paid whether they can capture the margins of running the service, but even if they can't, they still own the roads that you're driving on. So like they're getting paid either way. And so I think the data infrastructure companies, you have to really innovate way high up in the stack, because it's like being a fabulous semiconductor company. Like you can't actually control your destiny because you serve at the pleasure of one of the public clouds.

[00:48:46] JM: Man, I'd love to keep talking to you. We don’t have much time. Cool, man. We didn't talk that much about Material Security. Okay.

[00:48:51] RN: It's all in the website.

[00:48:53] JM: Thanks for coming on, man. This is great.

[00:48:55] RN: It’s a ton of fun.

[END]