

Take on Board

# Transcript – Nicola Nye on what boards should know about data protection



Helga Svendsen 0:00

Today on the take on board podcast, I'm speaking with Nicola nya about data privacy and governance. First let me tell you about Nicola. Nicola is on the boards of Fastmail, Correggio advisory group and is chair of tech diversity lab. She has previously been the chair of a scouting group committee. Nicola serves as Fastmail's Chief of Staff covering all areas of the company's operations, from overseeing their compliance and legal responsibilities to managing complex projects with external partners to building more effective internal culture across the global team. She's a firm believer in hope punk, cats, and chocolate. They all sound like awesome things to me, I have the cat under my desk as we are recording this. So I'm welcome to the take on board podcast, Nicola,

Nicola Nye 0:40

thank you. Hello. lovely to be here.

Helga Svendsen 0:41

So awesome to have you. And of course, we will delve into data privacy and governance in a moment. But before we do that, as always, let's dig a little bit deeper about you. So can you tell me a story about young Nicola, that tells us a bit about how you got to where you are today.

Nicola Nye 0:56

I love reading. And I'm well into, you know, books about superheroes and science fiction and all the rest of it. And I've always believed in right and wrong. And, you know, books always had the bad guys getting their comeuppance. And the heroine always triumphed, Justice was served. And it was bit of a traumatizing moment when my father revealed to me that, you know, the legal system does not mean that always has strong sense of karma coming back to take out the bad guys that the law was doing, its very best to embody these values. But often, the winner, you know, in a court case came down to who could argue according to the letter of the law, because we could not really necessarily hold people to the standard of the spirit of the law, despite our best efforts. And so fast forward a decade or three, and I've come through her my journey and technology working for a lot

of Melbourne's startup companies. And now I find myself here in this, this, these kinds of roles. And while other people might sort of shy away from law, compliance, governance and all the rest of it, I find it fascinating. It's a bit of a superpower to be able to dive into this stuff, and hold people to the kind of standard of that right and wrong belief that I had, when I was a children reading and getting into these books. And I believe it's a way that we can make sure that we build a better society, but build the thing that works the way we want it to work to make sure that the bad guys get stopped. And the and the good people get to triumph.

Helga Svendsen 2:17

Oh, my God, how fantastic that is not at all, you know how I expected a conversation about data privacy and governance to begin with our forces of goodness and evil and good. triumphing, that is fantastic. I like it was there were either of your parents lawyers, is that why that? No, no.

Nicola Nye 2:34

is a physics researcher, my father was chief financial officer. I just you know, got right into the storybooks. And off we go.

Helga Svendsen 2:42

Oh, fantastic. And dare I say it as someone who is a lawyer and myself, editorial comment, but it's also sometimes about the legal representation that you can afford. That wins out as opposed to what is what is actually right, you know, if everyone had the same access to representation, anyway, moving right along. So okay, so that gives us a bit of an insight. I'll look and I also sorry, just because I said it in your intro, hope, punk cats and chocolate. I'm pretty sure that most of the people listening have got a pretty good idea about what cats are. And I'm also pretty sure they've got a good idea about chocolate, both things very dear to my heart. You introduced me to hope punk recently, can you give us you know, the back of the envelope explanation about how punk

Nicola Nye 3:28

so you know, it kind of ties you know, I guess a little bit with they've got an evil story. And hope punk is the idea that in that punk sense of resistance and fighting back against, you know, oppression and kind of that regime that says you must conform. In modern years, there is a lot of bad stuff happening in the world and through the power of social media and global news networks. It can feel very constraining and hope punk is the idea that, you know, as an active sense of resistance, you can weaponize your optimism and fight back just by holding on to hope by shining that light out you can inspire others and through that generate change. And that in fact, it is almost your duty to, you know, fight back against this sense of repression, and show that there is possibility out there for

improvement and optimism in the world. And if you can inspire others and you can build a whole movement around it.

Helga Svendsen 4:15

Oh my god, you need a cape and to be flying through the skies going.

Nicola Nye 4:20

I will sign up for that.

Helga Svendsen 4:22

Fantastic Captain hope punk. That's what I might need to call you from here on. Fabulous. Oh, okay. Well, the rabbit holes I enjoy greatly about, you know, young Nicola, hope, punk cats and chocolate. However, we probably should turn to our topic of today, although it totally gives the context about why you told me the topic was data privacy and governance. doing what's right, not just what's legal. So, data privacy and governance. doing what's right, where should we start, Nicola?

Nicola Nye 4:52

It's a lot to dive into, I guess, to give a bit of context to data privacy, data privacy and the idea that that individuals have rights over data that other entities collect about them, really, I feel only entered kind of common knowledge when the Facebook Cambridge analytical scandal came out. And the idea that through data harvested out of Facebook, the outcome of actual governmental elections was being affected, and in a way that could not easily be reversed. And so people started to sit there and say, Well, hey, what data has been collected about me, should I be notified if that leak somewhere, we don't want it to go. So there's been a number of companies that have had data breaches and information has gone out. Obviously, once it's out, you can't put the genie back in the bottle, the most you can do is minimize harm. So the best thing you can do is prevent the breaches from happening in the first place. So this was sort of my first introduction into data privacy as, as something that the end user might care about, you know, everyday consumers should be aware of data privacy. But what I was finding through my work in technology was that a lot of companies were sitting there and saying, We think we've done the right thing, or we don't feel that we need to do anything more, or we need this data in order to further our business interests. I'm sure it won't be breached, I'm sure it's just fine. I'm sure all the partners, we're sharing the data with a totally doing the right thing with it. And I'm sitting here in the corner, rocking backwards and forwards saying you are just a nightmare waiting to happen. And so, you know, when serving on boards that you know, I think it's it's important to sort of sit there and say, look, you've got this great product or this great idea or this great service, yes, you can collect that data, it is legal for you to to collect that data, is it the right thing for you to to collect that data? Is there another way you could achieve your

goals without, you know, potentially taking on board more data than you actually need? Or using it in a bad fashion? Or have you done your due diligence with your suppliers to make sure that they really are going to use that data in manners in a manner that you think it should be? So that's, that's kind of the nutshell of data privacy. But maybe we should dive into a little bit more about data privacy itself. What does that even? What does that mean? And so you know, if you think about you go in, turn up at the library. Hi, I'm a resident on my local council, I would like a library card, so I can borrow library books. And the library will usually say, Well, you know, what's your name? Where do you live, what's an email address, and they need these points of data so that they can get funding for the government to prove that you live in the local area, they need an email address often so that they can send you fines or loan reminder notices. And they need to know your name so that they know who they're loaning the books out to. And if you don't bring them back, so that they can chase you down. But imagine they started collecting, you know, maybe they asked for your date of birth, or your hair color, or your gender identity. Or maybe they want to know if you're married, or how many other people live in your house with you. Or maybe they start talking to you about how many other libraries you might be a member of, or maybe they stuck in, you know, maybe they want to see your driver's license to help back up your claim that you live in a certain location. And suddenly, you can see that your humble local library might actually be collecting a quite a impressive treasure trove of information about you now maybe you know, your standard borrower, and then you have a car accident, and so you access their home delivery service. So suddenly, they might have medical knowledge about you as well. And if that local library has their treasure trove, and maybe they share it with other government departments, for the purposes of potentially getting the government funding, but the other government departments then share that data on and suddenly, their Work for the Dole scheme, people, that government departments suddenly might know that you're out of work or not out of work, because of you being in this car accident, suddenly, this data is being shared around against your will, against your knowledge and used for potentially justifiable reasons, but it might actually produce harm. And that's not even considering the idea that, you know, maybe the library's IT systems get hacked by someone nefarious, like a nefarious actor, and sharing all that data. And that's, that's a really simple example. Obviously, if you've actually got, like harmful organizations, like a lot of free software, like the social media companies, or someone like Google, you know, they've got to monetize you somehow, in order to pay for the service to be delivered. And so they are going to be going off and sharing your data and doing so with intent. As opposed to, you know, a library scenario where it happens accidentally, some companies are going out and doing this with intent, but just disgusts me.

Helga Svendsen 8:55

Likewise, I was, I was thinking of you recently, Nicola, I signed up for something I can't remember what it was. I don't know, maybe, and it was an event. And they needed what, sorry, they wanted my home address. And I'm like, there is absolutely no reason why you need my home address for this. But you couldn't register without having provided it. Ah, but I've just thought of it. Now. Why didn't I just put a whole bunch of gobbledygook in there? Because they generally don't test if it's real or not? Oh, well, whoever it was, I can't remember now I've given them my address, and I'll sell it off to somebody. Anyway. There's me sending myself down a rabbit hole.

Nicola Nye 9:30

Well, you know, you've had a really great defense mechanism for this. Someone from the Electronic Frontier Association, Justin Warren was saying, you can lie. Someone comes along and ask for data and you don't believe that they have a real interest cause for it, you can say tell them that your birthday is on the first of January in the year 1600.

Helga Svendsen 9:48

Like I think I by mistake did that somewhere once where I think I put my birthdate in is 1900 or something and I think it did actually ping say, you know, are you sure you seem a little old for this, whatever it was, so sometimes I've got them set up, but I've definitely, you know, put my phone number in as 0000, etc. And it's never been picked up. So yes, you can get around them. But I guess it's for us on boards, and I guess it's one thing boards might even be able to check is the integrity of the data. And if lots of people are providing 000, etc, as their phone numbers or providing, you know, meaningless addresses that are just x x, then for boards, it might be well, why are we asking for this data? What are we doing with this data? Is this data protected and held, you know, held securely? Are we selling this data? If so, who, too, all of those sorts of things is that the sorts of things boards should be asking themselves? Absolutely.

Nicola Nye 10:41

I mean, I would start with the basics, which is, are we charging enough money for our thing, such that we don't have to Ansel people's data, you should be proud to charge money for your product and service. If it's worth its salt, if you're on a board, and you think that it's good enough for you to serve on their board? Hopefully, they're able to make money from it and, and not have to sell it in order for you to be able to survive. So like, start there? And then second of all, is yes, you know, make sure that the team is doing their due diligence and, and reviewing what data are you taking in? are you storing it? Do you even need it? Can you write in a way that a customer can understand why you are recording this data, because if you can't explain it to a customer, it's a PR nightmare waiting to happen, which is really bad for your bottom line. And then you know, and that's assuming it just takes even one of your existing team to mention something in passing, where maybe a media outlet might hear or even just, you know, into the pool of your current customers, that's going to be all bad, it's going to produce a huge PR impact that is going to put your company in a world of pain and money. But then, you know, if you're collecting data that you don't need, and it is personal information, then if a malicious person does get in, then that's also going to be a huge problem. And it costs companies and can put them out of business, trying to make that right, because you need to go out and find all these people and tell them that this has happened and then find some way to apologize and make the situation good again. In Australia, we have mandatory breach reporting laws. So you actually got obligations under law, but you as a board member are going to be held to

Helga Svendsen 12:11

Is then every Australian organization like here, does it cover the mandatory? Is it someone who operates here, somebody who's registered here on the stock exchange? You know, what if they operate?

Nicola Nye 12:22

Yeah, what know the reach of it, but I do know, we are beholden to the FastMail is beholden to GDPR, and you know, any company that's selling services or products to people, EU citizens are beholden to GDPR, it's got its own breach reporting laws as well. And so you actually, you know, you might have exposure to these kinds of things in multiple jurisdictions, which is why for me, it's a bit of a gray area, I don't know the specifics, because fortunately for fast mine, we were actually GDPR compliant with GDPR came out, all we had to do was write some documentation to explain our existing practices. GDPR came out and a whole bunch of companies suddenly and abruptly vanished from the face of the earth the week before it came into law, because they had no way to make their practices compliant at all, what they were doing was totally dodgy. And they knew that, if that came out, and when that came out that they would be fined out of existence. So they just vanished a week before the law came into effect. So I, you know, I sort of actually not well up on the reach of our breach reporting laws, because we were just kind of doing it anyway. And, you know, I think, again, it's one of those, you might not be captured efficiently by the law. But the law exists, because it's a really good idea. You know, if you have a better on someone, and that data ends up in the wrong person's hands, you should go with them.

Helga Svendsen 13:32

Yes, yes. And it's, you know, as I said, back to the collection, it's like, lots of people are here talking about the security of data? And do we have the right kind of mechanisms in place, but it starts much earlier than that, like, are you collecting stuff just for the sake of it? If so, that's a risk. And as you say, you know, ending up on the front page of the Herald Sun test, it's a risk because you've got all this data that you didn't need anyway. And then someone hacks you or you sell it off, or whatever it may be, none of that is particularly good for your reputation and for risk. So it starts a lot earlier than some people think about it. It's not just keeping it secure.

Nicola Nye 13:57

And it's, you know, it's not just your data, it's you might have all the best reasons for collecting all the data that you have. But in today's society, most companies are not experts in every problem space. So they bring on other vendors, other partners to help them out and maybe with billing or website management, you know, maybe they're running their website on WordPress, or maybe they're using mailing lists software to send out their newsletters. So suddenly, you've got personal data about your customers, other things that are taking place, and you share them with your

vendors. So have you checked that your vendors are doing the right thing too, because if they have a problem, then it becomes your problem, because you actually were the one who shared that data. And so it's an organizational risk still, from that point of view. And this is why a lot of the times, particularly if you're a small startup and things you're trying to cut corners, you're trying to do things economically, things like the App Store, for instance, it has trained consumers and trained us even as individuals to look for free. It's been a giant race to the bottom. We expect things to be able to be free or cheap, and we resent paying money for it. And I think that sometimes particularly in that sort of startup ecosystem, you do look for how can we do this for free? Can we do it on the free plan? Can we do it on the cheap plan, or, you know, releasing the purse strings makes it really tough. But of course, if you're getting something for cheaper than it costs to run it, they're monetizing you somehow. And this can, again, impact on what you're getting up to. So you do need to pick good partners, and even having picked good partners, make sure that you know, you've got some good legal contracts in place to protect you if in the event that they get up to no good. So again, board governance, are all your partners in your ecosystem, also doing the right thing. So doing the right thing, when boards are looking at partnerships or third party providers, what should they be testing against to make sure that their third party providers are doing the right thing we're recently bringing on someone to do some stuff to do with our support system platform. So it was a plugin to that platform. And, you know, I went and had a look to see whether they had a privacy policy on their website that explained what data they were accessing out of the Support Platform and what they were doing with it, I had a look to see who they were using to host their data on where was it being saved and stored. I had to look to see you know how long they'd been in business. I didn't want someone who had just popped up six months ago and had a great idea. And then maybe we're gonna abandon it in another six months time. And then I wrote to them and I said, Hi, you know, we're beholden to GDPR, do you have a DPA that we can sign? And they sent me some data? And then I said, Look, you know, tell me about we want to use this aspect of your product. What information do you take on board? And what are you saving? And why are you saving it? And they were like, well, actually, we're saving everything. And I said, Why are you saving everything? You don't need it? And they were like, I said, Well, you know, you can save everything, we can protect that with a Data Protection Agreement. But like, if you don't need it, why are you storing it? And they said, Good point, we will, so great. So you know, this is this is the great thing about being in this governance position. And being so passionate about data privacy, and doing the right thing, like we could have done the base level, we could have signed it and just protected with legal agreements. But it was much better to have this conversation with the third party. And so you could do better here, you could just not store that data at all. And then you don't have a ticking time bomb. And we have much less concerns about our customers data ending up in the wrong place. Best possible outcome? Absolutely. That's actually customer taking an active role in it, although I check like you probably know a little bit more about this area than your average customer. Do customers care about this sort of stuff. I answered ticket support tickets, they come through and our support team escalates it up to us, because of fast mails, privacy stance, and being so critical of free email providers. I do get a number of inquiries from people and they ask detailed questions about you know, what kind of security we use our you know, is their data safe when it's in transit? Why are we not using particular things that they've heard about? Or they might write in about other laws that they've heard come in? You know, so yeah, I mean, I answer a range of questions. Some of them I get in often enough that I've actually got a sort of canned responses. And I'm like, yes, you're asking about this thing? Yes. Lots of people ask about this thing. Here's what you want to know. There is

out there in the ecosystem. There are people who are passionate about this just as, just as I am crazy, as we all are,

Helga Svendsen 18:10

It was from one of these conversations I had on the podcast. Gosh, more than 12 months ago, now that I finally got myself one of those password thingies you know the things a password manager. Thank you. That's it Password Manager thing. Best thing ever. Once you've got it all sorted, my lord, it took me quite some time, I was warned about that. And it does take you quite some time to get it all set up. But yeah, it's so maybe from this one, it will have to be as a consumer, I need to just take a bit more notice of those things. I actually read privacy policies, when they have click throughs. I read? I do mostly but I read them I don't sign up for whatever it was that people were asking details for. I was like, Are you just gonna Ansel this somewhere? So yeah, okay, that is a good reminder for me as a consumer to take a bit more notice of such things. And as a board director to think more about, I don't know if it's downstream or upstream, but the data does start with Do we really need it, then what's happening to it? And how secure is it? But do we really need that at the outset?

Nicola Nye 19:05

If you do the right thing, and not just the legal thing, but the right thing, and you're looking at your customers data, suddenly that becomes a selling point. Because you know, alas, in today's day and age, this is not yet standard. Privacy is not yet should be privacy should be the default. You know, surveillance capitalism should be the exception that requires special extraordinary circumstances for this to take place. We are not there yet. I continue the good fight and I'm waving my hope punk banner that you know, privacy should be normalized. But until that point comes along, it is probably going to be a competitive advantage for your organization to do the right thing with customer data and you can showcase to the world how good you are at looking after your customers data. And people will come to you because while they might initially aim for the company that maybe is the cheapest. One of the reasons that people stay with an organization is because they've got that value align. They've got they've got that warm fuzzy feeling that you know, I don't mind paying \$1 a month more or because the person at the cafe was nice to me or I really liked that they've got something that's burning diversity in the workplace on their wall. Or in this case, I really feel that they have my best interests at heart when representing and looking after my information that I am trusting them to hold on me. And that is you word of mouth referrals into new customers coming through the door, it produces stickiness. So even if something goes a bit wrong, they're like, Oh, well, you know, I know that they are trying to do the right thing. And you know, I've got this history of blog posts, or whatever it is about it, that has shown me that they're doing the right thing. I will forgive them this transgression and move on, rather than churning out at the first sign of trouble. So like, it's from a company perspective, doing the right thing. It's also hopefully going to earn you some new some revenue, well worth it. Kind of love that.



Helga Svendsen 20:42

Don't you win win? totally right. Oh, Nicola, I knew there would be way too much in this conversation. But we've covered a lot regardless. So what are the key things that you would like people to take away from the conversation that we've had today?

Nicola Nye 20:54

What is the purpose of the board, it's there to provide advice, and it's there to give your exec team and the company, some sense of external accountability, to hold up to the right standard. Because you know, left without that kind of accountability, it is easy to rationalize things. And I would say, don't be afraid of getting into that policy and compliance stuff, it seems scary on the outside. But once you start getting into it, you suddenly discover that it opens up a world of possibilities for you, it opens up marketing doors that opens up partnerships and relationships. And it means that you will get to know your vendors a little bit more closely and be a little bit more intentional about what the company is trying to achieve. It's pretty awesome. But mostly, like, just do what's what you can get away with Underlord, don't do the bare minimum, do the right thing. You know, pick the ethical choice, it might maybe cut back on a little bit of bottom line that you're getting up to certainly advertising in today's market is really hard unless you're using something quite intrusive, like Google Analytics. But if you do what's right, it comes back to pay you 1000 fold in terms of other things like customer referrals and sticky customer behavior.

Helga Svendsen 21:56

Yeah, loyalty. Nice. Oh, and is there a resource you would like to share with your take on board community?

Nicola Nye 22:02

Look, if you want to start looking into some of the data privacy stuff that is floating around, I would recommend looking at Salinger privacy blog, the team, their rights are really clear, easily able to be understood kinds of things. I would have a look at electronic frontiers Association. If you're not into advocacy yourself, but you would like other people to be able to advocate for you. They're a good group to get on board, check out tech diversity lab and fast mail for products that might help you.

Helga Svendsen 22:26

Yeah, fantastic. All right, we're gonna put links to all of those things in the show notes for people. And folks, if you're out walking, and you can't look at the links in the show notes right now just go and have a look at the website later, but we'll be there. Oh, Nicola. Thank you. So it's made me think Okay, so now after we've recorded, I will load this into, you know, my shared thing. And then what

do I do with the data there? When am I deleting? How am I getting rid of stuff, you've got my mind buzzing for my own organization, little and the ones I'm on the board of. So thanks for sharing so many great insights with the take home with me and with the take on board community today.

Nicola Nye 22:58

Absolute pleasure Helga. I'm very passionate about this. And it's a funny topic to be passionate about, but hopefully I have introduced a little bit of life into something that other people might shy away from otherwise.