Don’t Stop Talking PII, Start Putting Privacy Engineering into Action

Managing data privacy with a risk-based approach

Michelle Dennedy: You've heard us talking about privacy engineering before on this podcast, how it's foundational for developing technology solutions that preserve and protect information. But most companies have yet to adopt the privacy engineering methodology when building their own apps, devices or complex cloud systems or even noncomplex systems. This has got to change if we're ever really going to eliminate the threats to privacy and personal data. Which is why I'm so glad to be joined today by one of our true privacy engineering thought leaders, who scared me when I first met him, and we'll discuss that later.

Get ready to be inspired by some radical thinking that actually forbids the use of terms like PII, and helps bring a risk-based approach to how you manage data privacy across your organization. The revolution is now.

Cybersecurity, data protection, privacy. You like to stay ahead of the curve, and listen to experts who are leading the way in deriving greater value from data with a more organized approach to data privacy. You're like us, just a few deviations past the norm. You are a Privacy Sigma Rider.

Hi everyone, I'm Michelle Dennedy, Chief Privacy Officer at Cisco. Anyone who knows me gets that privacy engineering is something I am extremely passionate about. So you can imagine my excitement at being joined by one of the real pioneers in this topic. Ian Oliver is a Senior Security Researcher at Nokia Bell Labs specializing in high integrity entrusted network function virtualization tele cloud systems. Say that three times fast, I challenge you. He also holds a Research Fellow position at the University of Brighton in the UK and is now based in Finland, which is where we first met in person.

Welcome, Ian Oliver.

Ian Oliver: Hello guys, glad to be here.

Michelle Dennedy: He's a lot less shy in person when you actually meet him. We will draw you out of you. What really drew us ... And of course I'm joined by the inimitable Jonathan Fox.

Jonathan Fox: How is everyone?

Michelle Dennedy: He's back. As he’s affectionately known in the privacy community, “The Fox” is in the house.

Michelle Dennedy: Jonathan, of course, is our Director of Privacy Engineering and Architecture and Strategy here at Cisco. Long-time collaborator, and he attempts to be my adult supervision from time to time.

Jonathan Fox: Only when needed.

Michelle Dennedy: Which is every day.

Now, what I'll tell you about what scared us most about Ian Oliver is when my father, Tom Finneran, Jonathan Fox, and I published the Privacy Engineer's Manifesto in 2014, as soon as the book was in the can and any authors out there, you have no idea the relief and joy when the final edits are finally done or at least released, it's always more edits that you wish you would have done later. And then to find out that there's a book out there by this guy in Helsinki, Finland, called Privacy Engineering. And my fear was that here was going to be a book that absolutely disputed every theory we'd put forth, which shows you my confidence in our material. Fortunately, we were buoyed up by 32 other experts that contributed to that book. To my great joy, Ian didn't dispute our methodologies.

So what drew us to Ian was his book called Privacy Engineering, subtitled "A Data Flow and Ontological Approach," which introduces the concept of building information privacy into the entire product management development workflow. The idea is to include legal security and other organizational disciplines throughout the process to ensure full data privacy protection.

So Ian, tell us about that moment when you had finished your book Privacy Engineering, and along came the Privacy Engineer's Manifesto, and how do these books and works really interoperate?

Ian Oliver: Oh, great question. Well, first of all, I'm not scary, and two, one of the problems is you guys writing a book about privacy engineering, that was a big panic moment. Especially as I was late with the writing at the time despite it being self-published. Oh, what was it like finding out that you guys were doing that? Absolutely terrifying because there were some other people out there who were also doing privacy engineering, which I really didn't want. I wanted to be the only privacy engineer.

On the other hand, I was very happy that you wrote a book that approached this area, from a completely different angle. And it actually turned out we had two very complementary books. One written from the perspective of people who were trying to solve problem in the big ... In the large, if you like. I mean, little old me was actually just trying not to get sacked, just do my work better. The whole reason I wrote the book was because I needed to write down what I was doing everyday so I could repeat it and make sure I was doing everything properly, thoroughly, etc. I thought, hey, let's write all this, let's publish it and see what happens, and then you guys come along [inaudible] engineering.

Michelle Dennedy: And we were very much the same, trying not to get sacked and really trying to put down and make sense of a lot of the knowledge and ... It's interesting because I think we both wanted to kind of come up with some novel thinking, and yet we want this to be ubiquitous thinking.

Ian Oliver: Exactly, I ... What actually struck me ... Well, I come from a very, shall we say, deep scientific engineering background, and I was thrust into the privacy world where people were currently, oh, it's just legal compliance. You just point them to a privacy policy and everything is happy ...

Michelle Dennedy: Because lawyers are magic unicorns.

Ian Oliver: Yeah, and engineering is magic and it just happened because you think it's [inaudible]. I've seen systems that were in a pretty bad state, and people just didn't know how to get privacy ... I mean, the engineers I was working with were really, hey, we need to do privacy but we're not

reading 150 pages of legal text trying to figure out what requirements, just tell us what we've got to do. And I ended up orbiting these systems and I thought, wouldn't it be nice if we actually had a proper method to follow? Just give the engineers ... Show us some techniques. This is how you should communicate with the lawyers, and this is how the lawyers should communicate with the other guys. Show all the aspects, and this is how they all mix up to get them.

Basically, I just wanted to write down all the little techniques I was using, and getting these ideas that from ... Some [inaudible] couple of safety critical, the risk management world. The guys who actually kill people when things go wrong. Get all these ideas in because they were great ideas, and I thought this will be a great way of solving this problem. This is a great way of working, and you get some results, etc.

Jonathan Fox: Actually Ian, you'd be surprised not only are our books complementary, but I think our motivations were complementary as well. We were at the same point in our careers and our work with engineers where they were just expecting us to write a policy, or adapt a policy, or change a policy, or accept a risk on their behalf. And we realized we had to change how we spoke to them, how we explain things and move it into terms that they understood.

Ian Oliver: It goes both ways. I mean, my community, let's say the legal community, the engineering community, just to back double the really nice stereotypes and generalization, actually. Neither community were able to communicate to you. You got one side saying hey, don't collect personal data. And the other side going, what's personal data? It's contextual.

Jonathan Fox: Or what is privacy? And it's a big word ... and lots of components, and if you break it at a component level its manageable.

Ian Oliver: It’s actually led to the first revelation, which was let's stop using the term personal data.

Michelle Dennedy: I love it.

Jonathan Fox: I've moved to that, let's stop using the term privacy and let's talk about the components. So I think we're onto the same path.

Michelle Dennedy: Yeah, let's slow down on that one for just a moment. Did you just say, let's stop using the words privacy, personal data and PII? Discuss, gentlemen. Go for it, burn the house down Ian.

Ian Oliver: Okay, well first of all, what's personal data? And don't say everything because that's the classic answer ...

Michelle Dennedy: Exactly.

Ian Oliver: ... data.

Michelle Dennedy: Or nothing, if you're in a ...

Jonathan Fox: Or ...

Michelle Dennedy: ... A data center.

Jonathan Fox: ... The way things are changing, that will be the answer, unfortunately.

Ian Oliver: I mean, if we get stuck on this route of everything's personal data, let's go down this for a moment. Everything is personal data. Okay, so what happens next?

Michelle Dennedy: I'm imagining like a little tiny data knitting, like having little like hats, and little fuzzy wooly scarves for zeros and ones. Everything's personal.

Jonathan Fox: Well.

Michelle Dennedy: I wish you could see the look on the Fox's face right now ...

Jonathan Fox: No ...

Michelle Dennedy: ... He's like, what is going on?

Jonathan Fox: ... I'm looking at the little caps, but I agree. If we ... With our ability to analyze, do big analytics, to do data science, what not. More and more will become identifiable down to an individual.

Michelle Dennedy: I think that's true, but what happens functionally then, do we just all stop and slow everything down, and every decision is bogged down?

Jonathan Fox: I think this is why we need to let Ian continue.

Michelle Dennedy: Well, that's why I'm asking. What do we do?

Ian Oliver: If you think that the privacy officer comes in and says, okay you're handling personal data, and you choose a whole bunch of rules that you have to deal with, it doesn't really get you anywhere because the next question engineers will come back with, okay how do I handle personal data? Or they might come back with, we're not handling personal data, we're handling locations or identify ... The first things you realize that we social engineers is they don't handle personal data. They are handling less quantities of data of all kinds. I really would want to get across the point here that engineers do not collect data unless they have to. These systems are so damn complex to build in the first place, either won't be added complexity of security layers and privacy policies, and god knows what else we want to stick into these systems.

Engineers actually try and reduce things down as small as possible and keep it as simple as possible. So when you come up with a big term like personal data which means everything, we're stuck. We don't want to work with that, and it doesn't help us from a privacy perspective because a lot of the time the data that we currently use very, very necessary. A lot of the time it isn't the personal data, we're not collecting it for personal data reasons. We're collecting it because that's how these systems actually work. Further on from that and you get into this crazy argument after a while. If you question, what's personal data? The answer often comes back, well, it’s contextual. Well, that doesn't really get us anywhere because if the next question is, okay, can you give me the context? Well, the context is privacy and that's personal data. And you get into this whole nasty recursive thing which just goes around and around. Something, let's just do this, let's ban the term personal data from privacy.

Michelle Dennedy: I kind of like that. So the next go forward then is you take a risk based approach. Much is the general data protection regulation in Europe was written from a risk management perspective. What you're not suggesting is that we don't protect data. We don't create context for outcomes of systems. What I'm hearing you say is let's instead figure out what are these mechanisms and processes. This is how my legally trained brain is processing your engineered output. Is that ... Am I on track?

Ian Oliver: Absolutely, and if you look at the data that we are gathering and a lot of the data we necessarily have to gather, let's look at what it is and what its being used for. The first thing I was told by a lawyer when I was probably working privacy is, the [inaudible] is all about usage of data, which is very confusing because we're so obsessed with what data we're gathering. Not how it's being used. And I'm sure there's some lawyers up there that are going to attack me on that statement. I hope there are.

Ian Oliver: If we take a step back, you get into some very bizarre arguments after a while. You'll say, well, we're collecting identifiers and locations. Well, just because you're collecting those two data parts doesn't mean you're collecting personal data. But somebody will come along and say, right, its personal data because I say it is, and context, blah blah. It doesn't help us. We need to take proportionality to this, we need to be very specific about how we're handling certain kinds of data, certain types of data, and where it's being sent to. If you're not going to get down to those levels you can't have meaningful discussions, let alone minimization. You can't have a meaningful discussion of different kinds of identifiers and so on.

Jonathan Fox: And Ian, you also need to bring into the conversation then the reuse of data, because I think you know I agree. Primary use, a lot of stuff is collected and not necessarily ... It might be in some minds personal, but not used as personal data. But then it's what happens when someone wants to use it for something else? That's where the tricky stuff comes in.

Ian Oliver: Yes. If we don't know what that data is, then we cannot be proportional, we cannot have the applied correct anonymization techniques and we can't apply the correct kind of usage and protections, and so on. But we need to.

Jonathan Fox: Yes, and what you're really saying is you want to ban the use of the term PII or PI, or personal data, but you're not saying, don't understand what data you have. That's your point, is really understand what data you have and how you're using it.

Ian Oliver: Exactly, I mean if we hide behind the term personal data, we're losing so much context, we're using so much knowledge about how our systems are working, how we understand them. But it becomes absolutely meaningless as far as I'm concerned. We may as well just hide behind the gypsy policy and say, well what's the standard statement, every privacy policy we read we value your privacy.

Michelle Dennedy: We care about your privacy, yeah.

Jonathan Fox: And ...

Ian Oliver: Exactly, let's just hide behind that. It gets us nowhere.

Jonathan Fox: Agreed.

Ian Oliver: So the best thing you can do as a privacy professional, as a lawyer or as engineer is come to the point where you say, okay, what data are we holding? How much of that data are we holding? How risky is that data?

If you ask an engineer what data you're holding ... Well, just give it a look at high levels, they might say identifiers and locations. Well, your next question should be, what kinds of identifiers? What kinds of locations and what level of granularity? And have the conversation about the properties of the data, what it's going to be used for, how it could be identifiable, the longevity of the identifiers, the granularity of the locations, and so on. And all that information is lost if you hide behind the term personal data or PII.

Jonathan Fox: One hundred percent agreed. So how do you propose we move the two communities into a greater union, the legal and the engineering so that they do approach, if not talking the same language, talking a language that translates?

Ian Oliver: I'm sure at this point now there's a type of theorist out there who will be shaking his head vigorously at the next statement. I think we have to go to some kind of translation layer. Engineers spend a lot of their time working with machine level types, programming language types. But it's actually quite natural for engineers to talk about very high level, common sense things like locations, identifiers, sectional identifiers, application identifiers, personal identifier. There's a language that we can understand. Let's just work at that level.

If the lawyers just come down a little bit in their ... In the granularity of the conversation and the engineers try and abstract a little bit, you actually have this very easy, very natural middle ground of terminology.

Jonathan Fox: And I ...

Ian Oliver: And ... Yes?

Jonathan Fox: I was going to say I think it’s also important to change the nature of the dialog into more human understandable use cases as opposed to just engineering processes.

Ian Oliver: I'm glad you used the word process. I'd actually like to get away from processes too.

Jonathan Fox: Yes that's ... Yes, so that's why we need to get to use cases.

Michelle Dennedy: We're going to need a whole babel fish for the new language, and I like it. I'm sitting here writing notes to myself and I'm saying, you know this translation layer, and we're talking about lawyers, and we're talking about engineers. I think we're missing more disciplines in there, in this revolution ...

Ian Oliver: Oh ...

Michelle Dennedy: ... That we're priming.

Jonathan Fox: Yeah

Jonathan Fox: ... I've let ... Don't get it started.

Ian Oliver: When you start down this route ... I've worked a lot with one of these semantic web superstars. I'll mainly drop all the legislators, if you'd listen to the time. I've had to mainly drop lots of people ... Michelle Dennedy.

Michelle Dennedy: No, I know her. She's really dull. Who's the semantic web person that you were talking to?

Ian Oliver: Yeah.

Michelle Dennedy: Okay.

Ian Oliver: We worked a lot on defining these ontologies and then splitting them up and saying, okay, let's have an ontology that allows us to talk not precisely ... Not too precisely, but more precisely about what kinds of data we're holding, and what are the upper ontological types that we're getting in. Things like locations, identifiers, personal characteristics, timestamps. [crosstalk] ...

Michelle Dennedy: How did you get into the CN? I think it's fascinating because you are a highly technical person, and here you're talking about developing translayer ontologies with a semantic web pioneer.

Ian Oliver: How did I get into this? Oh, I'm a language nerd. I have a horribly deep interest in things like syntax and language, and

Michelle Dennedy: And heuristics.

Ian Oliver: ... Semiotics and semantics, and all this sort of stuff. So this is kind of a natural weird thing that happened in my career. I mean, I worked with the UML language back in the 90's before UML became famous for things like this.

Michelle Dennedy: We know that Tom and Jonathan and myself are ... We love our UML. I think it's some of this classic ... It's almost like there's classic reading if you want to know how to speak whatever your native language is. I think there's also classic ... And I won't use the P word for processes, but I think things like using anthologies, using UML, using cross disciplinary development, these are the things ... This is how we get better.

Jonathan Fox: Right.

Michelle Dennedy: This is how we radicalize and become pioneers.

Jonathan Fox: Actually, I just want to go back to a comment he made about we need to talk about ... Or perhaps you did Michelle, about more roles and responsibilities. And the fact is, privacy is becoming something with that if we have to have some acumen in across almost all domains. Whether UI, or customer experience professional, you're a marketer. The engagement begins far earlier with a system or a process than when you log in, and what really has to happen to improve our understanding about how things process and use our data is to really understand it as part of the total engagement with that. And so that's ... I like to talk about total product.

Ian Oliver: This is something that really ... I doubt we've tackled in any meaningful way as an industry. Do you remember the sort of 1980, 1990 of total quality management?

Michelle Dennedy: Yup.

Ian Oliver: You see a very holistic idea of a system. It's not so crazy after all.

Jonathan Fox: Yeah.

Ian Oliver: I think we're a long way from this ...

Jonathan Fox: Oh.

Ian Oliver: ... And we're still maturing as an industry. And I think that we're finally starting to have the discussion about the terms and terminologies that we're using in privacy, and the fact that we need different discipline roles within that.

Jonathan Fox: Yeah, and it's no longer something that is over in the legal or the compliance community. It needs to be front and center of so many different roles and responsibilities. There needs to be acumen across the board because each element has a role to play.

Ian Oliver: I can say something controversial.

Michelle Dennedy: Like we haven't already? Go for it, Ian.

Ian Oliver: I don't think we've been controversial yet.

Michelle Dennedy: Hey.

Ian Oliver: These privacies still too dominated by lawyers.

Jonathan Fox: That's not controversial with us.

Michelle Dennedy: Yeah, well I think that if anyone who's trying to hire a competent privacy lawyer right now months ahead of GDPR, and in the wake of GDPR afterwards, I think they'll tell you that feels very scarce for lawyers. But I will absolutely double down on your radical statement. I think it has been dominated by policy makers and wordsmithers, whether they're lawyers or not, and I think we need more art. We need more popular Dr. Who, Black Mirror, Twilight Zone explorations of the edges of what we want the outcomes to be. I think we need a much deeper and wider ontology and translation here.

This is actually the perfect time for this radicalization of privacy engineering I think, because I actually was ... To go back in time, looking at some letters between Ada Lovelace and Babbage, and looking at their different styles and their different ways that their brains were working to come up with really modern computing, and whether it was even one machine that does one thing, or one machine that does many things. Whether or not the outcome was stated in the beginning was a debate that those two individuals had back and forth across genders. They both

were in the same social class, but I think we need to have that cross generational, cross user, cross functionality type of radicalization.

So, in short to your radical statement, are there too many lawyers? I don't think there're not enough lawyers, but is there too big a proportion of lawyers? Yes, I think so.

Ian Oliver: Yeah, well I'm glad you mentioned Adrian Babbage. I'm glad you liked the book I suggested.

Michelle Dennedy: Yeah.

Ian Oliver: I mean, if we go back to Adrian Babbage ... I mean, what made that partnership rather productive was the fact that the period of the time actually allowed that.

Michelle Dennedy: Yes.

Ian Oliver: Whereas we seem to be with privacy ... We're not taking the bold step of, hey, let's employ an engineer in this ostensibly legal position. We're not making that kind of stats. I see evidence for privacy opposite positions and they very rarely say legal background required. Nobody's taking the radical step of, hey, let's just go and say put a whole bunch of mathematicians on this.

Michelle Dennedy: Yeah, and yet some of the greats ... I mean I'll call out our friend if we're going to namedrop, Jim Adler, one of the great privacy officers. He's now running ... I think he's the CTO for Toyota research, or something like that. But has been a privacy officer in his past. There're too many that I could name on one hand that are coming out of a traditional technical background, and so I agree with you. I think this is a revolution, and I think the other thing ... And I'll go back to Aden Adrian, I think it was a love affair too, and I think that we need to have a love affair with data, with the practice with innovation to really be radical revolutionaries here.

Ian Oliver: Yeah, I agree with that. And I think that's a very nice way of putting it. The question is, how man legal people are having a lover thing with data?

Michelle Dennedy: Not enough. We need to get naughty with our data.

Ian Oliver: Yeah, there's plenty of legal people getting very ... I don't know two lawyers get excited about contracts.

Michelle Dennedy: Scarily enough, they do.

Ian Oliver: I'll take your ... I've seen something. If you're going to go down this radical route, let's look at compliance as well.

Michelle Dennedy: Alright.

Ian Oliver: That's not such a crazy thing. Look at the GDPR. Look to organisms out there, take a good read of the GDPR and you realize, I think with quantity, really it's a very beautiful document in a way where it's been written from. It's been written by the [inaudible] people, and I've met some of these people and I haven't grade all of them. They decided to ... I don't really don't accept

subconsciously, or by design, but it actually says, don't do compliance. It says do with management, and that's a cultural shift that we're not prepared for.

Michelle Dennedy: So I'm going to say one more radical thing is, you know what I like about that? Is after the true shame of not having a federal law here in the US, I think we've been practicing risk management, the privacy pioneers in this country have. So I want to say there's a little bit of murky in there, in GDPR land.

Ian Oliver: I actually think that the people who wrote the GDPR have a background in the nuclear industry, the medical industry, the aviation industry because the whole thing seems to be written from this perspective that we need to collect data. You need to do this, you are going to be taking this risk. But beyond the processes and the techniques, and the tools to manage those risks.

Ian Oliver: I was at a conference back in November in Brussels about the GDPR and privacy engineering. Had a very long conversation with a set of gorses, who in the summary basically said, we need to learn from industries that've got their bad word together.

Ian Oliver: Am I allowed to say bad words in this podcast?

Michelle Dennedy: I do.

Ian Oliver: Okay. We need to learn from industries that have got their shit together. Meaning ... And this is the view I've been trying to push over for a very long time. The medical domain, the aviation domain, they've been through this process of bad things happen when we don't work together, when we're not being cross disciplinary, and so on. When we don't have a common language, when we don't do not take care, when we don't understand how our processes are working, how our methods work.

Ian Oliver: If you look at these industries, the reason why medicine and aviation are so safe is because they've taken a very deep look at themselves. They've gone through this sort of systems thinking approach, they've looked at the whole industry and realized that it's a mix of different disciplines. People with very widely different skills. It's only by having a common framework in which all these people operate and loads of other cultural changes as well. Boy, the culture changes are amazing, and that's how radical we need to be and I think the GDPR's the first step in this.

Michelle Dennedy: I love this. I'm getting frantic waving from our producing in the control booth that we've gone to 30 minutes, so I'm going to metaphorically ask you to land your plane with the medical folks and the aviation folks.

First of all before we forget, how do people get access to you, to your book, your online presence? How do they find you Ian, to get more radical on this issue?

Ian Oliver: The book is on Amazon. I would recommend you buy the Booksy version and not the Kindle version because Kindle doesn't do formatting well.

Michelle Dennedy: That's true, I have both versions. You want the paper. Pay for the paper, people ...

Ian Oliver: You want the paper one.

Michelle Dennedy: ... Don't be cheap here.

Ian Oliver: Yup, you can contact me by email, I'm on Twitter although my postings on Twitter are rather rambling. Do not contact me on Facebook, I will not answer. I don't use Facebook that much, sorry. Yeah, you can find me on Twitter, you can email me, you can buy the book. I mean, I could do with a second Ferrari.

Michelle Dennedy: Excellent. Yeah, and we're all getting just filthy rich on privacy engineering ...

Ian Oliver: Oh yeah ...

Michelle Dennedy: ... Radicalization. So ...

Ian Oliver: ... Absolutely.

Michelle Dennedy: ... I love it.

Ian Oliver: Spielberg called me the other day and wanted to film my ...

Michelle Dennedy: You too? That guy?

Ian Oliver: Yeah ...

Michelle Dennedy: Steve, my love. You know, Titanic was one thing, but privacy engineering, you're not ready. The world's not ready for that big of a blockbuster.

Ian Oliver: Yeah.

Michelle Dennedy: On that note, I want to thank you, thank you, Ian. And of course I'm going to beg you to come back on the show. We have to salute to all the names that we dropped today, Ada Lovelace, Adrian Babbage, and of course you know, how many ... We've already had a Norwegian death metal podcast, and now we've got Helsinki representing in the house. I think next European broadcast we have to do something from southern Europe, so we'll call you next time … and maybe start the film treatment.

Ian Oliver: Indeed.

Michelle Dennedy: And thank you, Jonathan Fox, for trying to ...

Jonathan Fox: Always a pleasure.

Michelle Dennedy: ... keep us in line as best you can.

You've been listening to Privacy Sigma Riders brought to you by the Cisco Security and Trust Organization. Special thanks to Kory Westerhold for our original theme music. Our producers are Susan Borton and David Ball. You can find all our episodes on trust.cisco.com or subscribe

wherever you listen to podcasts. Then please take a moment to review and rate us on iTunes. To stay ahead of the curve between episodes, consider following us on Facebook, LinkedIn, and Twitter. You can find me, Michelle Dennedy on Twitter, @mdennedy. Until next time.