Privacy Sigma Riders Episode 7: Eradicating the “Ick” Factor

Privacy Design and Usability

Host Michelle Dennedy discusses usability for privacy design with data science Professor Nathan Good, of Good Research and the University of California at Berkeley, and attorney Sean Butler of Emergent Law

Michelle Dennedy: Technology alone cannot possibly provide all of the solutions to its security and privacy problems. Human factors also play a huge role, and it's important for security and privacy experts to understand how real people interact with the systems they develop. This is truly what privacy engineering is all about. But how do you get a symbiosis between usability, security, privacy, ethics? Often, it has more to do with culture and whether your organization can accept that development might require a lot of research, planning, collaboration and person hours to build a better product or service.

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.

I'm very fortunate to have Dr. Nathan Good, and Sean Butler with me today. Hello, Nathan and Sean.

Sean Butler: Hi Michelle, thanks for having us.

Nathan Good: Hi Michelle, this is fun.

Michelle Dennedy: I'm gonna let you guys introduce yourselves. Sean, why don't we start with you?

Sean Butler: Okay. Full disclosure: I am a lawyer.

Michelle Dennedy: I'm sorry.

Sean Butler: I hope you guys stay on the call with me, on the show with me today. My name's Sean Butler; I am Contract General Counsel for startups and entrepreneurs. I was the General Counsel at Meraki for a number of years, both before and after its acquisition by Cisco, and I tackled a lot of privacy and security issues supporting that business.

Michelle Dennedy: And you currently have your own firm, right?

Sean Butler: Yeah, it's called Emergent Law.

Michelle Dennedy: See, you’ve gotta get that in there.

Sean Butler: Thank you.

Michelle Dennedy: And Dr. Good.

Nathan Good: My name's Nathan Good. I'm Principle of Good Research, User Experience and Privacy Security Firm, and I also lecture at UC Berkeley School of Information in the Data Science Program.

Michelle Dennedy: And his name is Doctor Good. It just doesn't get better than Doctor Good. What is Meraki, how did the two of you come to work with it and then work with myself and my team on privacy engineering stuff?

Sean Butler: Sure. Well, I'll take the first part of that. Meraki is an exciting, cloud-based, networking technology and a business, started in 2006. The typical MIT doctoral candidate story. Three guys from MIT.

Michelle Dennedy: I love that you think that's a typical thing, like yeah, you know, three guys.

Sean Butler: We're in a little bit of a walled garden here.

Michelle Dennedy: Coming to you from Silicon Valley.

Sean Butler: Born and raised and worked and raised. All that.

Nathan Good: That's right, you're originally Palo Alto based.

Sean Butler: I am, it was kind of a foregone conclusion that I was going to end up in technology. So Meraki started out building all the same networking hardware products that Cisco does, but the real innovation was the cloud-based platform that would manage all of the customers' devices and customers could manage, configure, deploy those devices through a web-based interface.

Michelle Dennedy: So you thought that you were going to be a lawyer there and not manage data points and data handshakes across networks? That's so adorable.

Sean Butler: Yeah, it wasn't too terribly long before I had my first security and privacy questionnaire to fill out and I remember, it was a wakeup call. I was sending out Microsoft word documents back and forth internally and finally one of the engineers got frustrated and responded, "It's 2012, we work at a startup, what does it take to get a Google doc around here?" I thought, okay, the world has changed for little Sean and now it's the new environment.

Nathan Good: That's right, because you were a big corporate lawyer before, right?

Sean Butler: Exactly. Started out at Wilson Sonsini. So Meraki's mission has expanded to beyond simplifying the network to simplifying IT and so Meraki's added, in the last couple years, both a phone and a security camera line of business to their platform. They're all still managed through, what they call, the single pane of glass. But you can imagine customers get a little concerned when they hear. They think, "OK, I'm buying a new network technology," and they hear the word cloud and they instantly think all of their network traffic is going to run through somebody else's cloud. So

we can get into the details of that more later, but absolutely, I was disabused quickly in the notion that I wouldn't have privacy issues to tackle.

Michelle Dennedy: Yeah, and I love what you're saying because, in all seriousness, it's amazing to me that in this day and age we still have venture-backed companies and private companies that have some sort of a mythical belief that they are not responsible, as a minimally viable product, for privacy and security. This is really is the linchpin of the value that a lot of these companies are providing, whether you think that you are a distributed service like a cloud, which still is the catch phrase for distributed services, or whether you're delivering something that's going to be on someone's actual company platform or in their hand or pocket as a telephone. It's a really important point that you bring out.

So Nathan, how did you come… what is a designer like you doing in a neighborhood like this?

Nathan Good: Yeah, that's exactly what my thesis advisers ask me when I started looking into this stuff a long time ago.

Michelle Dennedy: Now what was your thesis, now that you're going to tease me there?

Nathan Good: Oh, so I was looking at ways to providing usable notice and consent across various platforms. So we looked at ways of creating privacy controls, this is back in 2008, 2009, so at that time the idea of sending images over a phone was like, "Wooo, sci-fi." It's so funny because a lot of the stuff that I worked on in my thesis is now so prolific. At the time it was like, "Wow, why would you want to do this?" One of the things that we worked on, it was part of my original work, was if you're uploading phones to a cloud, how do you assign controls on that, how do you decide who can see it, who can't see it? Those kinds of things were part of that work. But, yeah, it's a weird space to be in. I kind of got into this, I started working on recommender systems back in the dot-com explosion.

Michelle Dennedy: What's a recommender system?

Nathan Good: Yeah, so recommender systems are, the ones that people are really familiar with, are if you go to Amazon, it says you may like this, or if you go to Gallup, it says you may like this or...

Michelle Dennedy: So this is some really good branding. It's a recommendation system that we're going to call a recommender.

Nathan Good: Exactly, exactly.

Michelle Dennedy: I like it.

Nathan Good: There's some really great… Malcolm Gladwell wrote some really awesome articles back in the day about the project I was working on, Movie Lens. A lot of the work in the beginning was really done around movie recommendations. Sort of what you see with Netflix and stuff like that. So, basically, what I started to see when we were working on recommenders, and this is during the dot-com era, is that there's tons of private information that a lot of these companies had that they were just not really doing anything with. They were just leaving on the floor, some areas had the key value for the database was a social security number, just really kind of strange

practices and it kind of rubbed me the wrong way and I remember talking to my advisers about it and they're like, "Yeah this is a big issue, it's something that you should start to pay attention to."

And then over the years, I remember just being more and more interested in it from lots of different angles and then finally, right around, I don't know, 2002 or 3, I wrote a paper. I was looking at peer-to-peer networks and saw that there's all this private information on it and I was like, "How is this getting on the private, peer-to-peer networks?" And it turns out that it was just a usability issue. So I wrote a paper about the usability issue that can contribute to privacy and security problems. And that was kind of the start of me putting together this idea of, "Well, this is actually really an end-user problem and this is something that we can really address with design in a lot of ways, as well as looking at things from the back end."

Michelle Dennedy: So, I want to slow you down a little bit, because there're a lot of concepts in there, Nathan. I think, that when I hear the word design, I typically think of, sort of end user being the consumer and window dressing, but the way I'm hearing both of you talking about this, it sounds a lot more like design for users that are using data, maybe in a company as well as users who are consumers, who are either donating or sharing intentionally their data or even observation systems where we're observing and recording. So, when you think about usability, how do you dig in? So how do the two of you put your, what are the legal constraints, what are the design constraints together, when you're thinking about this issue? And I'll toss that out to both of you guys to kind of, how do we dig in? This is complicated.

Sean Butler: I'll just jump in with one of my favorite examples from Meraki that I think gets to your point. We've got multiple categories of users and each one with its own relatively defined or undefined sets of goals. One of Meraki's products is called Systems Manager. It's a mobile device management software. It's Meraki's only software-only product. It allows enterprise customers to manage fleets of mobile devices whether they're laptops or smart phones, using that same central interface.

Michelle Dennedy: I like the visual of a fleet of phones. It's kind of like they're all sentient coming together.

Sean Butler: They were going to call it iRobot but they thought that was a little weird.

Michelle Dennedy: Oh dear, no trademark problems there at all.

Sean Butler: What they're finding is, early iterations of mobile device management were largely what you could call command and control. The enterprise customer wanted to be able to completely lock down these devices for security and privacy reasons and protecting proprietary information.

Michelle Dennedy: And we've seen how locked down corporate information is.

Sean Butler: Yes, exactly. What they experienced in, one of the fun parts of the collaboration Nathan and I have done is, vicarious experience through the Meraki product teams mirrors what trends and dynamics that Nathan has seen in his own research. They realized that if a device is locked down through command and control, the actual individual user is just not going to use it. So they say thank you for my locked down company phone, I'm going to stick it in this drawer here in my desk and I'm going to find ways to check my email on my personal device.

Michelle Dennedy: So the information is even less protected if you're being overly prescriptive and not thinking about the user.

Nathan Good: Yeah, absolutely.

Michelle Dennedy: Right, right.

Nathan Good: We call this, in my world, sabotage. And there's some great examples. One of the favorite examples is...

Michelle Dennedy: I just call it stupid. But I don't have a doctorate.

Nathan Good: Yeah, that seems a little judgmental.

Michelle Dennedy: I know, I'm judgey.

Nathan Good: One of my favorite examples of this is when this one company, I can't say who they are, but they decided, okay, we're going to give everybody key cards because we want to know when everybody comes in and when everybody leaves.

Michelle Dennedy: So cute.

Nathan Good: So they instituted a command and control of head of module because they wanted to keep track of their employees, but then what started happening is managers were using the amount of time that companies were at, that employees were at the company, sort of to say, "Oh, you're working harder or you're working longer." So what ended up happening is this massively competitive, it was already competitive to begin with, that just got unattainable. Basically, all of the people who worked there would have to be there 16 hours a day.

Michelle Dennedy: And if you looked at the data, everyone was there 24/7 because everyone's then swiping cards in for their buddies and things.

Nathan Good: Exactly, but what the solution that the users came up with to deal with this sort of untenable situation was brilliant. They basically elected somebody to carry everybody's key cards. They gave everybody their key cards and then everybody went in, clicked in the same time and clicked out the same time and then that person would rotate and that's how they did it. So, what happened, is because of these external uses of this data that eliminated the trust that caused this really uncomfortable situation, they circumvented the entire point of the security measures in order to just get work done. That's one of my favorite examples of this thing that Sean's talking about, like sabotage.

Michelle Dennedy: It's an elegant example because if you look at a privacy-engineered system at its finest, you start with the objectives, that the system is supposed to at least assist, if not pamper, and then you design from there all the way through including these context diagrams of who is doing what to whom and for what reason. And what you're saying is, we can't now, if there's a fire in the building, we don't know who is in there, we certainly aren't managing well, and I've seen this key card game before where poor managers will pull security badge data to assess the amount of time someone was physically present in a geographical location and what I've always advised

over the years as a privacy officers in various companies is, you don't need more badge data, you don't need my permission to get badge data, you need to buy a pizza and get some comfortable shoes. That's my technological fix.

Sean Butler: So true. And that's reflected in Meraki's approach to mobile device management now. Their priority is really to come up with a product that the individual user actually wants to use because it helps them feel more confident about the way they're using company data.

Michelle Dennedy: So they want to use it.

Sean Butler: The media involved ratcheting back on the command and control, which feels.

Michelle Dennedy: The Martians are coming.

Nathan Good: It's going to get hot today, for those of you who are not in California, we get emergency alerts if it's going to be hot because our weather's so perfect, I'm sorry. Hate me, it's fine. But it's going to get a little hot this weekend.

Michelle Dennedy: I kind of like it in there. Can we leave it? OK. We can edit that out, but I kind of love it. So guys, I love what Sean said about users wanting, I mean you're talking about a sociological and a psychological phenomenon. How do you join that to actual systems that you're building and designing and then making sure that they are within legal constructs? How do you meld those worlds of humanity living within architecture and architecture living within humanity? Not that that's a small order in the next two minutes or so.

Nathan Good: I can talk a little bit about some research I've been doing, collaboration with a research group out of Berkeley, specifically around the BYOD space and mobile device management.

Michelle Dennedy: That's bring your own device, yes?

Nathan Good: That's right, yeah, thanks. Bring your device. And certainly to Sean's point of, how do we get people to really enjoy this? One of the things that we've found is people are generally concerned about all the things that are happening on their phone but they don't really have a good way of controlling it. So they acquiesce and they say, "Well". There're lots of different strategies they employ but they try their best to sort of manage these within the scope of what's reasonable for them. But often times what's reasonable isn't enough. So, at Berkeley, in conjunction with ICSI, we've developed a system that allows people to manage stuff a lot easier. And we provide...

Michelle Dennedy: Did you just say ICSI?

Nathan Good: ICSI yes, International Computer Science Institute. I hope I got that right.

Michelle Dennedy: It sounded like Tinkerbell was landing, so I wanted to make sure ICSI got its full due.

Nathan Good: Yeah, absolutely. I mean Tinkerbell can get pretty upset sometimes. I have kids and I've watched the cartoons.

Michelle Dennedy: She's rough.

Nathan Good: She can be pretty nasty; we don't want to upset Tinkerbell.

Michelle Dennedy: Nope.

Nathan Good: Yeah, I think, what we've sort of found is we created a way that both uses the system architecture, as well as, the machine learning and really simplifying the choices in interface design so that users can make better choices in line with their context and expectations. But we found that they're pretty happy with it and so sort of to Sean's point earlier about making people happier about having controls and happier and more comfortable providing security, there are ways to do this and there's an entire research field on usability, security and privacy that lots of really talented people are looking into as well.

Michelle Dennedy: I'm really excited. I want to underline too, as I often do on this podcast, that we have engineers that are fun and talk about Tinkerbell and we have lawyers who are talking about making people enjoy their systems. So, I just want to underline that. We're busting stereotypes as we're building really innovative new products. How did you guys form this partnership with each other?

Sean Butler: We actually met in grad school in one of the most enjoyable parts of law school for me, it was a bit of a refuge, at the time it was called the Samuelson Technology and Public Policy Clinic.

Nathan Good: I always forget which one goes first, is it Public Policy or Technology?

Sean Butler: And Pam Samuelson is a fantastic professor. She teaches both at the law school at UC Berkeley and at the Information School, where Nathan got his degree. And she founded a public policy clinic as a result of her work in the early days of software-related cases and the early extensions of copyright beyond source codes to object code.

Michelle Dennedy: I love that. It's like a privacy clinic. I've often thought that I needed a twelve-step program.

Sean Butler: Well, it was a real eye-opener for me to even consider the notion that there might be a public interest in technology and that's, I think, well, I won't speak for you, but that is, as I have worked in the private sector, that has always been in the back of my mind thinking, "Okay, we need to make sure we have trust in place with our customers, otherwise there's really nothing, so I can write you whatever ridiculous legal terms you want me to write here, startup colleague, but unless your customer trusts you, we really don't have a platform on which to proceed."

Michelle Dennedy: It's so true. So, I'm going to wrap up our conversation. I think we could go on and talk about design and I would love to have you guys back on the show to talk through some more use cases. But kind of the closing point that I'm trying to ask everyone, what gives you hope? What gives you hope about where we are today? Do we still have hope in something called privacy and security and trust?

Nathan Good: I think from my perspective, over the past couple of years many things have given me, I guess what you call hope, I guess what I call motivation to keep doing this. Probably the strongest one for me is just the students I have in the Data Science Program. The course that we have is an

elective; it's not required, but it fills up every semester and it's not something they can take to their boss and say, "Hey, I took Privacy Ethics," and it doesn't come across as very technical, but the questions that they bring and the enthusiasm that they have for the topic and their willingness to sort of really engage with these issues and bring them into to the organization is just to me, really exciting. They talk about real issues and they talk about really exciting work that they're doing and these are data scientists who are going to be building our future.

For them, I feel that we have a real obligation to dig into these topics really deeply and provide them the information and the tools that they need. And one of the things that they always tell me is, "Well, after I've taken this course, now what do I do? And how do I engage this in the workforce?" And I think that's on us as privacy engineers to really give them the tools and give them the ways of engaging with the product, which is why it's so great to have someone like Sean that I can refer them to and say, "Hey look, Sean is this legal department that most of the time you guys are trying to avoid." And Sean has this really great moniker, they call themselves “team buzz kill”, sort of tongue-in-cheek, which I thought was fantastic.

Your legal department really wants to understand what's going on and you can think of them more as a team rather than somebody you have to get around. I think that's one of the things that really gives me hope. They're taking this course and they're looking at what we’re doing and they're saying, "Oh well, the problems that the legal side are engaging with, the problems that I have to engage with and the privacy problems and the social problems are all the same thing and we can all work together to really address these.

Michelle Dennedy: I love that. So Sean, take us home, what gives you hope?

Sean Butler: You know, I think what gives me hope is working hands-on with, there's my experience working hands-on with the people who are building these products and I think the more ubiquitous technology becomes, the more granular the use case and how we use it. The people I see building the products are themselves immediately turning it around and thinking, “Well, if I was going to use this product, what information would I be comfortable transferring to the service?” I always talk to people in terms of the “ick” factor. OK, again, I can write you various sets of terms but is there an ick factor here? How would you feel using this? And most of the time these days I don't have to ask that question more than once. In my experience, people are starting to answer that. Developers are starting to answer that question more and more on their own.

Michelle Dennedy: So we're evolving away from the ick.

Sean Butler: Yeah.

Michelle Dennedy: I love that. Well, thank you guys so much. I think we've just barely scratched the surface of your true Sigma Rider-ness. I hope that the takeaway for everyone listening is, you know this incredible partnership between computer science, design, legal, advisory for startups. Startups can do this, startups that are bought by huge multinational companies can continue to foster that beautiful product that you've built or service that you've enacted after acquisition. I think that these are really important parts to note that when you're doing privacy engineering, when you are a privacy sigma rider, it has worth in your community, for yourselves in your careers as well as commercially. So, where can listeners get in touch with you guys? Nathan, you will not

brag about yourself, please at least say the name of your wonderful book that I've read many times, and how do we get in touch with you and then, Sean, how do we get in touch with you?

Nathan Good: Sure, so I'm Nathan, just nathan@goodresearch.com. You can get in touch with me there. The book that Michelle is referring to is Security and Usability: Designing Secure Systems that People Can Use.

Michelle Dennedy: Soooo good.

Nathan Good: It's edited by Lorrie Cranor, but...

Michelle Dennedy: Who I'm desperate to get on this podcast, by the way.

Nathan Good: Yeah, she's fantastic. It's a great primer for people who are looking for a lot of information about some of the ways that usable security and privacy research has been created and evolved.

Michelle Dennedy: And so, Sean, how do we find you?

Sean Butler: I just recently started my own consulting business and you can reach me at Sean, S-E-A-N at Emergentlaw.co, or find me on Twitter @SPButler.

Michelle Dennedy: He's very good, but I get him first, just so you all know.

Nathan Good: He's fantastic and if you're good he may give you a team buzz kill tee shirt.

Michelle Dennedy: I need a team buzz kill tee shirt! Well, thank you guys very much, and we've got a white paper about the privacy impact of Meraki cloud services coming soon. It'll be available for you on Trust.Cisco.com.

Nathan Good: Thanks for having us.

Sean Butler: Thanks, Michelle, this was great.

Michelle Dennedy: 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.

Related Links

Trust.cisco.com (Meraki white paper coming soon)
Emergent Law
Good Research
Cranor, Lorrie Faith, and Garfinkel, Simson, editors. Security and Usability: Designing Secure Systems that People Can Use, O'Reilly Media, 2005.