Privacy Sigma Riders Episode 1: On the Road to Trust and Data Privacy

Cisco Chief Privacy Officer Michelle Dennedy kicks off the Privacy Sigma Riders podcast series with a conversation with John N. Stewart, SVP and Cisco Chief Security and Trust Officer.

Michelle Dennnedy: In 1965, the amazing computer science pioneer, Grace Hopper, predicted that someday information would be more valuable than all the hardware that processed it. That day is here. It's estimated that one billion gigabytes of data are generated every day. That's trillions of dollars in value over the next decade. But what if I told you that 75% of that value will be dependent upon people's trust in our collective ability to handle data securely and to use it ethically and responsibly? Cybersecurity, data protection, privacy. We like to stay ahead of the curve and imagine increasing the value of data with novel approaches to data privacy. We like it out here on the edge -- just a few deviations past the norm. We are Privacy Sigma Riders.

Hi everyone. I'm Michelle Dennedy, chief privacy officer at Cisco and your host for Privacy Sigma Riders where we talk all things data privacy and protection, with some of the world's leading thinkers and doers in the field. Why Privacy Sigma Riders? Imagine a world of standard curves. Everything is hot, sticky, and sweaty underneath that curve. It's where about 80% of the world lives by definition. What we're going to talk about in this series are the people who live on the edge. The people who live on that standard one, two, or three deviations from the norm. These are Privacy Sigma Riders. This is a place where we talk about values, like personal privacy and how we convert those values into valuable data assets. We'll talk about engineering privacy and to your products in your corporate culture. About philosophy, ethics, leadership, and organizational prowess. Hopefully, we'll have a lot of fun along the way.

I wanted to open our first episode with a nod to Grace Hopper. Not only is she a personal hero of mine, but she invented the very first compiler. She taught the earliest computers how to recognize English words and symbols, and convert them into machine code. In other words, she developed the first systematic approach to programming that simplified what, until then, was a slow, complicated process. This helped speed up the task of programming and reduce the number of errors. More importantly, it freed programmers from the mind-boggling task of speaking binary to focus on their true objective, solving business problems. That's exactly what we need to do in data privacy. The business value of data is clear, but confusing and often conflicting regulations and evolving customer expectations are making it more difficult to use that data.

So much so that data has become a game of risk versus reward. On one hand, businesses want to be free to use the data they collect to create new and rewarding user experiences, make smarter decisions and increase revenues. At the same time, consumers are demanding that companies treat their personally identifiable information as if it were their own. Why shouldn't they? At Cisco,

we view privacy as a fundamental right as well as an asset. It's an individual's right to define and live their life free from unwanted intrusion, exposure, or observation. Data privacy for us then refers to the way we process, use, manage, analyze, share, and treat information about individuals according to fair, moral, ethical and legal principle.

Even the best intentioned companies can go astray of consumer trust and the law without a thoughtful, systematic approach to privacy protection. I coined the term privacy engineering to describe just such an approach. It was first introduced in the Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value − a book I co-wrote with Jonathan Fox and Tom Finneran. It's a process that uses traditional engineering concepts like business activity and process-flow diagramming to build systems that respect identity and data about people. Like Grace Hopper's compiler, privacy engineering helps translate vague concepts of policy into concrete specs and requirements that are understood and actionable by designers, developers, and anyone else within the privacy ecosystem. But don't let the term fool you. Privacy engineering is not just about technology or the products people buy or consume. It's also how you operationalize privacy. How you run your business with a privacy mindset and organize around your business.

That's why I am so excited and pleased to introduce our first guest, John N. Stewart, senior VP and chief security and trust officer, who is something of a cybersecurity celebrity in our world. Welcome, John!

John Stewart: It's good to be here. Thanks, Michelle.

Michelle Dennnedy: Thank you for coming. This should be fun. John, you and I talked two and a half years ago now about the team you were building as Cisco's chief trust officer. Before that time, Cisco obviously had been doing a lot of compliance things and working a lot within the legal teams for privacy, but you never had a formal privacy officer. What changed and why did you feel it was time to add someone to your team? I'm a little afraid to say, why me John?

John Stewart: Confluence of events. I think certainly you and I were talking about it at the time, but for everyone else not in those private conversations we were having, we had moved into an era as a business which was no longer about building hardware and software, but actual data systems running operations in other corporations. Going into a multinational domain of building and operating. The custodial nature of all the information that we had collected was something that we had to stare pretty hard at and up our game internally to protect data. The switch was we had to go to a much more [external and internal] combined point of view. We had to set reasonable expectations of what we think being a multinational IT and systems and communications provider is about; how we would formulate the world's thoughts on how and what was practical for us as a business and what was practical and operationally possible in this day and age.

We've changed as a company. Add in the fact that the world, as you know all too well, is also changing simultaneously. The level of scrutiny of companies, providers, and multinational companies all increased at the same time. Then never to be underestimated is when an industry leader becomes available on the market and you try and figure out how to get her to come into the company.

Michelle Dennnedy: I'm glad I did because we're having some fun over here. For people who may not know, it is kind of a new job category. What's a chief privacy officer to you?

John Stewart: I think it's really important to have a person that wakes up and goes to sleep and thinks about them as a fulltime job. Certainly, privacy is not my area of expertise. To answer that question, it's basically the person that wakes up, goes to sleep, is an expert in that field and is committed to making the differences that are necessary. Both intra-corporation, so certainly to Cisco, but also, you've been doing this for a long time, you've also been an individual advocate outside whatever company you worked at, between the various businesses you've worked in. You've always been an external advocate security, just like I have. Combine all of those together and it's the person that wakes up, goes to sleep thinking about it all day long. Intends to make other people think and pay attention to it all day long, and then advocates throughout the industry that this is an important topic and here's how to approach it. In fact, in no small part, it’s the reason I think you're doing this podcast.

Michelle Dennnedy: Exactly. Someday I will sleep at night but ...

John Stewart: Not yet.

Michelle Dennnedy: I do think about data all the time as you know. It's pretty remarkable really. It feels like it's yesterday for me too, but you and I were talking as I was trying to build out a culture of data protection and privacy. Before that was even a thing, you were already thinking about secure connections and the relationship of security to really empower people rather than to lock stuff down. Today at Cisco, we have this brand promise to securely connect everything to make anything possible. How did you manage to get so many to come on this journey with you? How did you capture the hearts and minds of the company to really go and execute on that vision?

John Stewart: Ironically, at the time of this recording, I was just celebrating 15 years of when John Chambers and I were actually talking about the transition of Cisco to be a major security player and now, arguably I suppose we’re certainly in the top two. Maybe even in many categories, the number one leader in the business of security. The discussion was not about firewalls. It was actually about taking an industry position on what the network could do and what our obligations as a result of helping build the internet looked like to shaping the future of it going forward. The challenges we were thinking through certainly were how to build a multibillion-dollar security market, but also, what would Cisco have to do to change ourselves in order to be ready for that?

The second aspect of that was building a world class security team. You and I know this naturally because we've worked so long together, but the word security was not the word security. It was a combination of resiliency and data protection and privacy and certainly operational "security" and infrastructure security. It was this amalgamation of a whole bunch of things and it couldn't just apply to security for security's sake. It had to be security as a broad thought process throughout anything we did. If we built a phone; if we built a firewall; we ran a web service; we bought an online services company; it had to be embedded to get scale. The first thing I did was to ask John to be a part of it, if not lead it. I'd rather have the CEO stating "this is the culture of the company and this is what we expect" and as the CEO at the time and now chairman, he embraced that and said it's everybody's responsibility.

In fact, it was one of his first quotes out the gate to his leadership team. Then you start measuring the efficacy of that. You start building up instrumentation that says, "Okay, we're making progress. We're taking a step back. What are we doing right? What are we doing wrong?" Things like just only five years ago, I would tell you that we didn't have a data-focused protection team. We had data protection. We looked for loss of information, but not a data-focused protection team. And it was started where the largest set of data was in the company and then we just branched out from there. How do you get people aboard? First of all, you ask the CEO who's got a bigger title than you do and then the CEO does it and then it's really easy to get people aboard.

Then the next thing is you start measuring and you start showing progress and how it's going to make a difference internally from internal metrics. Never to be underestimated is the fact that you use every single customer expectation on your company to force the changes that need to happen through examples. Verizon was a terrific (and still is) a terrific customer of ours. AT&T was pushing us. They weren't pushing us because they thought we were doing something wrong. Their expectations were rising and we had to rise to meet that.

Michelle Dennnedy: It's very cool and it's all about building. I think that's really the focus on this whole podcast is how do we build things together? Not how do we tear things down, what are we afraid of? What goes bump in the night? With that in mind, you've talked a lot about metrics and culture of what is, in the broader sense, what does winning look like to you? Is it 100% compliance or is there a bigger objective here?

John Stewart: I think the only way you get to 100 ... First of all, it's not 100% compliance because bluntly I think if you get to 100% compliance, the compliance level is either too low, you're wrong because you actually haven't looked at it right, or you've hit this miracle moment which is going to disappear the next moment because data is in motion, systems are in motion, people are in motion, and requirements are in motion.

Michelle Dennnedy: I'm imagining a little cartoon guy going, "Hooray!" Then a rock rolls over him.

John Stewart: See? Exactly along those lines. I don't think of it as that. What I think is really success is when trend lines are going in the right direction and you're well aware of where the areas that aren't going perfectly are actually operating and in essence, you've created this bound condition that says, "Okay the business to achieve its needs on behalf of the customers who expect us to do what they have asked us to do and achieve those goals is fully aware of where it's going well, is aware of the fact that it's not going to go perfectly, so be ready for when it doesn't and then takes the risks that are commensurate to the risk acceptance of the corporation knowingly. “Knowingly” being a key word. Then transparent. Talking to your customers exactly like you have done. It's astonishing to me that we're trying to achieve something perfect in a world where there is no such thing.

I don't think you should strive for anything less, but I don't think you should ever expect you're going to attain it. I go for the trend line. The trend line is you're heading up and to the right. You've got more people involved. They actually understand what you're talking about. They've become ambassadors and empowered to do what they need to do in order to help the goals that you've set out. Then you just get out of the way and start showing what the measurements show which is that you're heading in the right direction.

Michelle Dennnedy: It's very cool. I think one of the fun things about it is there are some parts of privacy and security that have to be precise. You want to keep the malware out. You want to keep the ransomware at bay for sure. You also kind of if you're doing things right in my mind -- and what I'm hearing from you, John, is you want to be a little messy. You want to be able to grow with your customers. You want to be able to change with your culture. You want to be a little fluid here. You don't want to be so restrictive and imagine a place of perfect.

John Stewart: Correct. Look, if you're not fluid, your business is probably not going to be around. That's the other thing I always remind myself is the shareholders own Cisco and the customers are the reasons we exist. Those two groups have very big expectations that are translated through the board of directors and the senior leadership team ultimately onto all of us. What I don't believe is the case, though, is that you create such rigidity that the motion that you're in right now says, "Okay, this is all it's going to be and we're going to hold everything back and that's going to be it," because the pace of innovation, the pace of business, frankly, has just moved way beyond that. The way that you get through that the smoothest is you embed it into the business process.

You and I have talked about this certainly in the past, I remember the days (and I've been in the security industry for 30 years) where the security person was in the back. They were like, "Oh my good grief, please don't give them Mountain Dew, feed them pizza, let them out of the cage. Certainly don't ask them a question because they're going to say no anyway even if it's" ... How do you spell the word yes? No. That's basically how that looked a long time ago. Then it was IT starting to take this cooperation between security and IT. And I think we're still struggling through that phase, but ultimately, every bit of the word

security, privacy, data protection, resilience and everything else should be embedded in business process. Then it's just naturally and smoothly moving with the rest of the pace of the company. That to me is a pretty good destination to at least head for.

Michelle Dennnedy: I like it. You sort of touched on this already, but I think for some listeners, they can look at us and go, "You know what? You're Cisco. You have a dedicated trust officer. You live and breathe this stuff. That's your dedicated job." Whether you're a worldwide technology leader, a born-in-the-cloud newcomer, a 200-year-old manufacturing firm who's recognizing and waking up to the data reality that data is driving the new economy. It's critical for everyone to get this risk-reward thing right. Get to building this into their cultures. What advice would you give to others who want to embark on a similar journey? How can they make this work for them wherever they are in the journey of cybersecurity, information management, data protection, privacy? What would you say if you weren't you?

John Stewart: Well…

Michelle Dennnedy: I guess that's kind of an impossible question to ask.

John Stewart: I was going to say that pretty much is impossible.

Michelle Dennnedy: We're getting very existential here, John.

John Stewart: I'll get back to you on that when my alternate reality clicks in and I can answer your question.

Michelle Dennnedy: There's a Tardis showing up later, so it's all good.

John Stewart: Perfect. Excellent. I would say this. It seems like it might be easier at Cisco because we're Cisco. It's not. There's 70-odd thousand-plus employees, $45-plus billion-dollar business.

Michelle Dennnedy: They all have opinions too, I find.

John Stewart: They all have got great and very valuable ones by the way. Then there's the multinational nature of our company that we have to be thinking through all the pros and cons of what we have to get done. I actually long in some cases for the days of having a five-person company that's got a data reality and can just have a room and that's it and we all know where we're going. What I would simply say, though, is don't try and do everything. What you're going to want to do I think (and I still think our team practices this all day long), is set a strategy over a period of time and then say, "Okay, this is what we're going to do for now and this is what we're not going to do." It's impossible to do everything. It doesn't matter if I was given all the money in the world. I still couldn't achieve

everything we wanted to achieve because the amount of time to do it or the number of people to do it aren't available.

We just apportion. In my case, thinking 15 years on end, there were phases of our development where if you'd looked at us 15 years ago, you'd have been like, "Oh good grief. You don't have half or a tenth of what you probably have now." At the same time, I was facing that reality in 2002 and it didn't feel easy just because I was at Cisco. In fact, it felt pretty hard. Then it was just a matter of sort ordering. You just started and went somewhere and then you iterated and went somewhere and iterated and built and built and built and built and built. When I see an artist who's painted an amazing painting, then ask them how did you do it, they said, "Well, I first put a little bit of paint on and then I just kept going." The outcome looks amazing. It's something I can't do, but when I listen to that point, it's like, "Oh right. You just started." That'd be my advice all the time. Just start.

Michelle Dennnedy: I like that. It's like data art. That's really good. A couple more soft skill questions for you. Taking some time off this summer, I hope you had have some time to relax. Any sort of flashes of insights or things that are top of mind now that you're sort of fresh and fall is upon us. What's top of mind in that fresh brain?

John Stewart: Part of what is I think top of mind in just wandering in various countries and even just spending time with family is that there is an incredible population around the globe that in some cases knows (and in most cases doesn't) that they're depending on all of us to try to do this right. For the most part, wander through the world not knowing that it could go wrong and have probably never met any of us that are actually trying to do it right. Some of that's just the gravity and reminder that there are just so many people that really, really do want us to do this right although they don't even know it. That's number one. Number two is that you spend time with various friends and family and you remember that it's gotta outlast you. It's gotta be long. It can't be a Michelle Dennedy result; it can't be a John Stewart result. It's gotta be a business and a global and a group result and team win and that kind of thing.

Then that naturally leads me towards who are the next five of both you and me that we can find? That's when you spend time with the interns that work at Cisco and they just give you all this energy. Then you look for people that are remotely curious about this stuff and you bring them into your circle and go, "Please be interested and come onboard." Then the final thing I think that I have definitely landed on is I've had an appreciation for the way business is going and how fast it changes. I think the sobering reality is that no matter how fast we even feel like we're going at Cisco, it's still too slow. I don't want to fear that. Some part of me was reacting, especially during vacation, going "Man, I'm pretty tired already. I can't imagine going faster." Then a part of me sobered up and said, "Okay, wait. It's not about speed for speed's sake. It's actually about efficiency and about decisioning and quick iteration and all the things that'll get you to a faster state without necessarily making it feel like more work."

Those are the three that I took away. I can promise you that you and I will be in staff meetings after this podcast that we'll talk about every one of them because it'll be the pace and focus areas for us as a team and you and I working together as we usually do.

Michelle Dennnedy: Yep. It's exciting stuff. On that note, perfect last question for you, whether it's security-related or not, given all of these challenges, big and small in the world we find ourselves in today… it's a big messy world, what gives you hope? What are you thinking about in the bigger sense?

John Stewart: Always I would tell you that the thing that has given me hope every single day is the number of people that I get to know, get to meet, certainly get to work with in your case. Add yourself definitely to that list, that are committed to the fight and to get through it and make it better and actually do something good for the world. That will always give me hope. In fact, it consistently doesn't matter what all the bad news is as long as I know that there are people that are really pushing towards doing the right thing be it protecting their family, protecting their country, protecting data, protecting a company, protecting customers, trying to change the market of the industry, make a mark, use leverage of a company of our size to help privacy and data protection in your case, be something global. That gives me a ton of hope.

The second thing is I think of hope really as it's a little bit of a destination. I think frankly just positive outlook is an extremely smart thing to have in life. I'm not naïve to know there's all this other stuff going on. I just don't let it control my outcome and control our destiny because that's the intellectual horsepower that can override anything which is that you're actually approaching it with a, "Okay, I know what it is. I gotta go do something." If you ever want to know where I got that from, you can talk to my dad because my parents were instrumental in making sure that's the way I think.

Michelle Dennnedy: Well, I've talked to at least one of your kids and I know that you've handed that down too. You continue to inspire me and my girls every day.

John Stewart: Vice versa.

Michelle Dennnedy: John, thank you so much. This has been really huge and I hope every listener takes away not just how do we do this, how do we approach this at Cisco but hopefully you picked up some tips on leadership, on life, on remaining open to the challenge and you stay optimistic. We've got a big fight on our hands and I know we're going to win this one. Thank you, John.

John Stewart: My pleasure, Michelle. Thanks a lot for having me today.

Michelle Dennnedy: Remember that statistic I mentioned at the beginning of the podcast? Seventy-five percent of value derived from data will be dependent upon trust? That was pulled directly from Cisco's Midyear Cybersecurity Report. It's a great read and

will help you stay ahead of the curve and the latest cyber threats. You can download it free at trust.cisco.com. Thanks for listening to Privacy Sigma Riders, a production of the Cisco Security & Trust team. Our producers are Susan Borton and David Ball. Special thanks to Kory Westerhold for our original theme music. You can find all our episodes on trust.cisco.com or subscribe wherever you listen to podcasts. If you're listening on itunes, please take a moment to review and rate us. 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, ride to the sigma, riders!