Building Trust in the Digital Era

Data privacy, information security, and cyber defenses have the same goal: to achieve trust that will sustain electronic commerce and create value. Achieving digital trust is a competitive differentiator for winning.

Michelle Dennedy: We're so caught up with the immediacy of data privacy, we're finally superstars. Especially now, with GDPR in full swing, we often forget about the impact of trust and how that impacts our future technology development. How can laws like GDPR, the Japanese law, the new Canadian refinements and so on, influence tomorrow's systems and software engineers? What learning principles are being applied today to continue the transformation around us, and really talk about and measure trust? There are some really smart people thinking about how to best leverage trust for the good of privacy and for business. Today, I am super excited to talk to one of them who's helping shape our next generation of computer science geniuses. Stay tuned.

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 approached to data privacy. You're like us, just a few deviations past the norm. You are a Privacy Sigma Rider.

Hey everyone, Michelle Dennedy here, chief privacy sigma rider at Cisco, and someone who's always looking to continue her education, particularly, as it relates to new advancements in trust technology and development.

On this podcast, we tend to speak of here and now. What's trending in data privacy, how new GDPR and other laws will impact business here, etc. But, how is trust influencing our future? How are today's college students leveraging privacy design principles to make improvements in the way we communicate and rely on digital assets? Pretty heavy stuff, and something my special guest and dear friend, Jeffrey Ritter, is helping to drive as a visiting fellow at Kellogg College at Oxford University. Yes, you can get a mini, mini taste of Oxford University here on the podcast.

In addition to being an external lecturer in Oxford's Department of Computer Science where his course on governing information is part of the software and systems engineering graduate program, Jeffrey is also the author of Achieving Digital Trust: The New Rules for Business at the Speed of Light. Not just a teacher, Jeffrey's professional journey includes nearly three decades in private legal practice and active leadership roles within the ABA and United Nations to build a legal framework for global electronic commerce. Welcome, Jeffrey Ritter.

Jeffrey Ritter: Well, thank you so much. It's a pleasure to join this terrific podcast series you've been developing, and I hope that I can provide just one small contribution that may be helpful to your audience and to the people that are trying to build privacy in today's world.

Michelle Dennedy: Yes, definitely, and I hope to suck you in on many future episodes, because there's no way we can cover your amazing book and all of the great ideas and platforms you've already laid out just there. Thank you for coming and at least giving us a sample. You and I started talking about the

idea of digital trust years ago. Tell us a little bit about yourself and how you really came to developing this methodology of looking at digital trust and starting to measure it and really break it down into something useful.

Jeffrey Ritter: Well, it actually began a long time ago in a land far, far away. When one of my first clients was an American retailer that wanted to send faxes to their Chinese manufacturers for retail women's garments, and they wanted to make the fax real so they didn't have to put a sales person on a plane all the way to Beijing where the Chinese were insisting on blue ink signatures on real paper. The question was, how can we make the digital record of a fax to be real? Yet, with every new generation of technology, that client and many others started coming back to me and asking, "How can we make this next new thing just as good as the real thing?" Whether it was from fax to electronic data interchange, to electronic mail, to the newfangled thing called the internet and all that has followed.

I realize I've always been trying to find the answer to the same question. How do we trust digital information? In fact, this issue was part of the debates on privacy much longer than many privacy professionals realize. As early as 1990, just a couple years after the '86 directive. In the negotiations with the United Nations, the European Union was battling with me to push into a standard practice for any contract that required compliance with the data privacy directive, on a global basis. I've been dealing with privacy and trust for a long time.

Michelle Dennedy: Yeah, it's really interesting too. I mean, and we think about trust and data and imposters. Right? Someone that gets on a plane who you've never met in your life, and you didn't have Webex technology at the time, gets on a plane, walks in a room, and signs with a pen with blue ink in it on a piece of paper, and we trust that. We say, "Ah, now we have an enforceable deal." Then you try to get to this place where, what would it be to get you to that same feeling and enforceability in the digital world?

I think there's a lot going on there about identity and representation and expectation, and cross-cultural expectations that you're pointing out, again, with the United Nations being involved in trying to figure out, how do we build privacy into our systems? Take us a little bit forward. There you are working with the ABA and the United Nations. How did you end up getting this all put together into achieving digital trust, and then currently your role at Oxford educating graduate students?

Jeffrey Ritter: Well, to be very candid, by the year 2006 I was so perplexed by the question that I had to step away from the practice of law and just focus on the question and the answer. It turns out that, despite all of the research that has been done on trust, whether it's an organizational management theory or human interpersonal relations or the classroom between teachers and students, the model that I was looking for had not been created. To be very honest, I reimagined what is trust as a predicate to being able to figure out what it means to achieve digital trust.

Michelle Dennedy: How do you mean that as different from security? I think a lot of people listening think trust is synonymous with security. I don't think it is and I know you don't either.

Jeffrey Ritter: It's a good question and it's a fair one that a lot of people have struggled with, particularly in trying to make the economic justification for why we need to spend more money on security. I think that the differential is in where we place the presumption. Security takes the beginning

presumption that all data is true, and what makes it invalid are the compromises or the hacks or the other behavior of malicious actors that degrades our way of, basically, adding things up to trust. With calculating trust, it takes a different perspective, a different mindset where we almost begin at zero and ask, "How do we gain the trust?"

When you think about whether you're going to evaluate a teacher that you're going to entrust with the education of your children, a business partner that you're going to do a joint venture, or someone who will be a custodian of your personal information, you don't start at 100%, you start at zero. It is ultimately a mathematical calculation that's occurring between our ears. We have rules. We look for those rules to be populated by information we gather, and it is only when quite literally we can get things all to add up, that trust is the outcome.

In many respects, I think security has for nearly the two and a half decades that I've been involved with it from a legal and technology perspective, started on the wrong foot. Instead of advocating for the money to be managing risk, we should have been advocating for money to invest to improve the trust our customers, the data subjects with whom we interact place in our business, because it's only with that trust that we can create more wealth in the business. That's how businesses grow, is when people trust them.

Michelle Dennedy: Yeah, and I love this because you're also implying organizationally, the way current organizations run, when you talk about trust as you said, and I've advocated this for years too in that, what retailers and other kind of first time interactive business, it's like going on a blind date. You might have a little bit of information, but you're not going to go in there and go, "Oh my god, I have this boil. It won't heal. It's on my left buttock." You're going to go in and say, "I'm wearing my best outfit. I'm on my best behavior. I'm showing up in a way that I'm going to try." Why? To incur trust.

It's similar, you know, you have a physical person walking into a retail, they've seen something that they like about your store; it's clean, it's got pretty something in the windows, there's something they've heard about. It's kind of reminding me that your security and your technology teams are doing one thing. Your marketing teams, your business development teams may be not connecting. How are you connecting this concept of data as an asset to go into your teaching model for things like trust decision models and unified rules and information model? All of these are huge concepts. How do these two forces come together to start with zero trust and build?

Jeffrey Ritter: Well, ultimately, I think the answer is, we begin with the money. If I was to say to you that I have a wonderful flying apple, and I have an apple for every human being on the planet, then you're not necessarily going to care about how much you pay for that because everyone has access to it. If I only have one apple and it's unique and that apple isn't a fruit but perhaps a medical record of my entire medical history over some 60 years ...

Michelle Dennedy: Or even time — just time to browse something.

Jeffrey Ritter: That has a separate value; it's unique. What we're discovering is that if we treat data as property, something that is bought, something that's sold, something that's created, something that's stolen, the valuation of that as something that has some equivalent value in money is

what makes the difference. Building trust in our digital information is all about understanding the connection between trust and how we make money.

When we make that shift, the conversation also shifts when we're talking security versus trust, because now I can have whatever complicated two factor authentication with biometric encryption of data with a token, and most CEOs won't care what the technology is. If I walk in and say, "Sir, what we're going to do is use these technologies to produce 15% greater loyalty in our customers, producing 8% greater revenue because they will trust the confidence with which we collect and apply the personal information to better meet their needs," the CEO is going to say, "Done," because we've shown how the business is succeeding.

Michelle Dennedy: Yeah, he didn't get past "We're going to make 15 percent more," to be fair.

Jeffrey Ritter: Right. We're not spending money to prepare to fail, which is what security is often arguing in trying to justify their budget.

Michelle Dennedy: Right, or preparing so that no failures occur, so you're preparing for silence. I want to flip back a little bit. We're following the money, which I think is always a healthy thing to do in business because it tends to be highly persuasive with investors and backers. I also think it's interesting that we're assuming scarcity, which is a basic economic principle. Then I think, how do you get by the backlash against this notion as data as property? Where, on one hand, advocates of "it's mine," they lose the model and the narrative of "it's ours," because we've had this conversation together, that time belongs to you and me and anyone who's listening, versus as you've said, an ephemeral asset, data as property that fits into the scarcity and monetary model. How do you reconcile that nut?

Jeffrey Ritter: I think there's a tool or an approach that I can suggest in response. We often talk in business about a risk reserve. Right? We need to put a certain money aside for the banks that's required by the Basel international standards, so that if bad things happen we can recover. We have resilience within our business. It could be money we've spent on insurance. It could be money we set aside to pay lawyer costs or settlement fees. Or, it's what we have to put aside to recover from a security incident.

Jeffrey Ritter: On the other side of business and the economics of business, there's something else that, frankly, I have not seen discussed in economic literature, which I've called the trust discount. Let's say that the news last night had a story that rat turds had been found in the manufactured raisin bran of a major manufacturer.

Michelle Dennedy: I just like that I didn't bring up rat turds, just for the producers in the studio. Thank you, Jeffrey Ritter.

Jeffrey Ritter: You're welcome. On your way home this evening, you've got to pick up a box of raisin bran. You go to the store, and one box is sealed with colorful marketing on the outside, but the other product is a transparent cellophane bag that allows you to verify that at the bottom of the bag there really are plump, juicy raisins.

Michelle Dennedy: So many thoughts in my mind right now.

Jeffrey Ritter: Let's imagine that the price of the cellophane bag is 20 cents more.

Michelle Dennedy: Right.

Jeffrey Ritter: What you would pay for that and the difference is what I call the trust discount, because the transparency is allowing me to have confidence that the vendor and the product are worth what I'm being asked to pay. In privacy today, as we've all seen over the first two, three decades of network based communication, the information has been swept up from us. Every interaction, including the phone number that you call, somewhere is being recorded. For us to move forward on privacy, and for any of us in a global competitive marketplace to survive, the consumer is going to be making choices about which vendor, which service supplier they can trust, and what they are willing to pay.

If that personal information is being collected without the transparency that the consumer can calculate, they're going to pay less or they may choose the competitor, even at the same price, if there's a higher sense of confidence that the rules will be followed. That gets fascinating, because it comes down to what I'm so excited is in the new GDPR, which is the principle that the system that will be respected under the law is one that has been designed well, that actually has the rules being considered at the front end of the engineering as opposed to a patch that gets applied only when the bad actor took advantage of the flaws or inconsistencies in the systems.

Michelle Dennedy: It's an interaction of two of your concepts that I hear you talk about a lot. One is mobile rules and the other is the velocity principle. Can you briefly tell us what those things are, because I think that's what I'm hearing around this transparency and the built in-ness required by GDPR and some of these other rules? Which, you know, anyone who's listening to this podcast, if you don't know what the acronym for GDPR is you should probably go back to a prior episode, but for those of you who don't want to do it, general data protection regulation coming out of the European Union. Sorry, that's what I was hearing is, mobile rules, velocity principles, and how they fit with design and transparency.

Jeffrey Ritter: Just so everyone knows, it was May 25th in 2018, I was finishing my class at Oxford and actually ordered and presented to the class a cake celebrating happy GDPR day. We saw in this law this principle that, for data to move across systems there has to be, in effect, a confidence that the rules and the terms of collection that the data subject originally agreed upon in their consent are moving with their information.

Mobile rules has nothing to do with mobile phones. Instead, it's the notion that, when data is created it will, particularly with personal information, be immediately controlled by the consents and permissions and rules of engagement between the data subject and the original collector. Once that data moves downstream into other processors, the data subject's concern is that their permissions and controls are going to be followed and respected as the data gains mobility across the system. Mobile rules is a way of thinking it, when I build my design around that PII when it's first collected, I can pass those rules through. In effect, the rules carry with the data through the complexities of cyberspace. What this presents us with is a challenge.

The second thing you asked me to talk about was the velocity principle. Business is inherently successful when it moves faster. We know that velocity has risk. One of the key things we're looking at (at every layer of engineering systems today) is how can I squeeze more time out of a

process? How can I improve its latency so that things move faster? Well, it turns out that as data is moving across systems, much like personal information, every time it hits a new port or a new gateway within a system, it's much like a traveler coming to a customs officer crossing a national border. You stop and you're inspected. Is this safe data? Is this malicious code? Has this information been collected pursuant to the right rules for us to receive it and process it? That takes time.

The velocity principle is one of those things that it's easy to say, and yet, I think it has tremendous implications for how we design effective privacy controls. It says simply this: the velocity of information is proportional to the transparency of its governance. When information's moving, if I can't tell you where I came from and when you ask me questions of whether I've been in West Africa and I can't answer those, I'm not going to get through the border.

At the same time, every packet of information, including things that are tagged as PII, faces the same challenges. The ones that are going to win and the PIA that I will have confidence in providing because of the systems downstream are connected, are the systems that can show the performance data, the log information, and essentially the compliance that our systems have executed of the original consents and permissions of the data subject when the data was originally collected. That's velocity. The winners are going to be the ones that figure that out.

Michelle Dennedy: I think that's right, and I think as data borders become more porous it will be up to the designers of these systems and the business leaders where we can follow the money. I want to kind of close on this great feedback you got at the end of your Oxford class, so I'm going to brag on you a little bit my friend. That, you know, they thought that digital trust should be something that is absolutely required for any software systems engineering degree.

I couldn't agree more, and I think it's a combination of, you're not building a system that's going to run in a university laboratory. You are going to be having information about other human beings, about business, about things that we care about, about assets and trust, traveling with velocity across these very fluid open and mobile borders. I loved that feedback and I will double down to anyone who will listen. If there are any Oxford dons listening right now, we need Jeffrey Ritter who does not yet have his PhD but I will grant him a virtual one. You have a Sigma Rider PhD. I will call you Dr. Ritter, because I like it. How about that?

Jeffrey Ritter: Between you and me, that's fine. Everyone else can just call me Jeffrey. The key thing here is that many of the concepts that companies have embraced in picking up security and trust together, and creating trust officers, and Cisco is one of several companies that reoriented this, already understanding that the learning principles we gained over 25 ...

Michelle Dennedy: My marketing team is in the room, by the way, cheering for you right now Jeffrey.

Jeffrey Ritter: Twenty-five years of privacy management are actually informing this, how we will also govern and regulate our industrial data. All the other incredibly valuable data assets of business that are not PII are going to need the same kind of engineering and design principles that people like you and other pioneers in privacy have helped us understand and have matured over the last 25 years.

Jeffrey Ritter: As we look at the next generation, it's exciting to think about that privacy design principles are not only going to help us better define who's the winners and the losers in the management of personal information, but will also help inform how we create a more robust and more economically productive cyber environment for all digital information in business. Ultimately, information is our fuel and the stuff that will rise to the top, the cream of industrial data will be the information that companies have governed with the same principles of design, execution, transparency that we've sought for personal information.

Michelle Dennedy: Absolutely, could not agree more. People that know me well and know what we're working on under the covers, I never ever think about PII in isolation. We think about data and we think about it on every one of these levels. A lot of takeaways. I think the one thing I will take away and offer to our listeners, Jeffrey's published a lot. He's got an article in the Duke Law and Technology Review, as well as of course, pick up his book Achieving Digital Trust: The New Rules for Business at the Speed of Light.

I think it is a rare and wonderful, delightful thing to have a Durham, North Carolina-based Kellogg College Oxford University visiting professor as a show guest, but most importantly, as a friend. Thank you, Jeffrey, for all of your insights today, and I would love to have you back on the show so that we can break down some of these big, hairy principles and start living with some data velocity.

Jeffrey Ritter: It would be my pleasure. You know, one of the things that is so impressive to me is the optimism that my students have expressed for the importance of all these topics. One thing that I haven't had a chance to share with you is that, last Friday when I finished class, there's the normal polite applause from the class which is fairly routine in many graduate classes. Something happened that was absolutely unique and very humbling. The first student getting up from his desk decided not to go out the door, but to walk toward me and shake my hand and to express his thanks personally. Then he actually hugged me. Then, Michelle, every other student in the class comes to do the same.

Michelle Dennedy: In England, these are not huggy people.

Jeffrey Ritter: Each of them expressed their appreciation for the course ...

Michelle Dennedy: I love it.

Jeffrey Ritter: The excitement of what they had learned. They are actually coming from four continents. It was coincidentally in Britain, but not many of the students are British.

Michelle Dennedy: Yeah, yeah.

Jeffrey Ritter: I think that there's excitement here, it's global, and it's important that we keep the dialog going so that we keep moving that ball a little bit forward in terms of improving all of our trust in all of the systems of the cyberspace.

Michelle Dennedy: I love it. Well, thank you again Jeffrey. From the Sigma Riders, where we love talking trust, velocity, raisin bran rat turds, it's a wrap.

Jeffrey Ritter: Thank you.

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.