# SM191 | 8.24.2024
# Summer Playlist 2024 | Episode 7
## Michelle Finneran Dennedy, CEO, PrivacyCode.AI

**Our Summer Playlist rolls on this week with Michelle Finneran Dennedy, CEO of PrivacyCode.AI. David Greely sits down with Michelle to discuss privacy in the age of data as a highly valuable commodity – and the focus we need to be putting on data supply chains and the data industry in the wake of the National Public Data breach.**

---

**Michelle Finneran Dennedy** (00s):
I think by having a law that says we're going to start by you telling us what is your data strategy. Do you have an architecture? Do you have someone who is accountable at the top? So I do think we need something that's broad enough to allow accountability, but also broad enough to continue to invite that innovation that will help us protect for the different types of businesses that have to flow.

**Announcer** (26s):
Welcome to SmarterMarkets, a weekly podcast featuring the icons and entrepreneurs of technology, commodities, and finance ranting on the inadequacies of our systems and riffing on ideas for how to solve them. Together we examine the questions: are we facing a crisis of information or a crisis of trust, and will building Smarter Markets be the antidote?
This episode is brought to you in part by Abaxx Exchange, where trading in centrally cleared, physically deliverable LNG and Carbon futures contracts is now underway, ready for smarter markets.

**David Greely** (01m 08s):
Welcome back to our Summer Playlist 2024 on SmarterMarkets. I am Dave Greely, chief Economist at Abaxx Technologies. Our guest today is Michelle Dennedy, CEO of PrivacyCode. We will be discussing privacy in the age of data as a highly valuable commodity and the focus we need to be putting on data supply chains and the data industry in the wake of the National Public Data breach. Hello, Michelle. Welcome back to SmarterMarkets.

**Michelle Finneran Dennedy** (01m 36s):
Always a pleasure. I can tell it's summer because I get to talk to you.

**David Greely** (01m 40s):
Well, I am glad that you do. You know, and I was reading the papers the past couple weeks and I am realized that the bad news is that a breach of privacy and data security are back in the headlines. And the good news is that you are back on Smarter Markets to help us make sense of it all the headlines of course have been on the national public data breach, which has led to 2.7 billion records containing social security numbers and personal information on potentially hundreds of millions of people being publicly released on August 6th and I was hoping you could put that breach in context for us because at a headline level, it seems massive how much damage has been done?

**Michelle Finneran Dennedy** (02m 21s):
The quantity and the quality of the damage in this kind of situation is over time. So right now I think the immediate damage is more spectral than actual, but I think there is sort of two mind thoughts here. One, why aren't we talking about this more? Why aren't we hearing all the commentators being afraid, wring their hands, et cetera, et cetera and I think it's partially because we have become numb. We keep hearing about breach after breach, we are spending trillions of dollars on security measures and security leaders and fancy C-suite designations for people and yet we continue to have these massive bunches. So the other side of this is it's a massive bunch. I mean, we are talking about billions of records. Unfortunately, I think this is the beginning of an era now that we understand that data and training data and data supply is a market, a new market that is allowing for this boom town of ML and AI. This is the beginning

**David Greely** (03m 36s):
And I want to come back to that with data and the market and this huge new demand coming from AI with you. But first I wanted to go back because National Public Data from my understanding, is a company that aggregates and brokers data in this data market for use

in background checks, you know, employee background checks, criminal background checks and now while the headlines and the hand wringing such as it's been has been on the public release of this information, I am equally concerned that a private company had all this information in its database to begin with all those social security numbers on hundreds of millions of people. So what's going on here, Michelle? Why don't I hear the same level of concern that a private company had all this data that I hear about it being made public?

**Michelle Finneran Dennedy** (04m 24s):
Absolutely, and you should be concerned, and this is data brokers themselves have been the subject of many, many congressional hearings and certainly a lot of hand wringing. I think there is a couple of layers of concern here. One is if you are using this background check service is your expectation that they retain all of that sensitive information and I don't think that is the expectation. That's a matter of contractual understanding between companies that hire these groups. I think that's kind of red flag number one on the play for me, should you have this much data, it seems wildly disproportionate to whatever services you are offering. So you are a legislated outside of the US based on proportionality and the weight and in many of the states now that we have a series of state laws, this is disproportionate as far as I can understand as a far outsider.

**Michelle Finneran Dennedy** (05m 18s):
I have to give you the disclaimer. I don't have any inside information about the nature or character of their architecture or controls. But what you can see simply from the reports on this breach, they are hoarding data. These are data hoarders. I wouldn't even call them data brokers because data brokers should be having command and control of the various types of data. We have a bunch of different tools and capabilities so that you can anonymize certain kinds of information. So that concerns me a lot. Like from the outside, if I was a regulator red flag on the play, the controls simply do not seem to be in place to reduce the attack surface of the risk. The other side of the coin, and I have heard this one hundreds if not thousands of times from colleagues over the years where folks are concerned on quote unquote risk.

**Michelle Finneran Dennedy** (06m 10s):
So they are looking at data and what is at risk. The first thing they talk about is intellectual property. Well, I used to be a patent litigator. I can tell you it's very expensive to litigate intellectual property. Trademarks are very valuable. Copyright and software always a mushy topic, but valuable and you see a suit every 10 years or so that kind of lifts your eyebrow. Why are we not considering personal data about the most important element of any business? It's people and the question is kind of this shoulder shrug of well, it's just employee data or it's just a credit card number and you can replace your credit card. So it's sort of layer on layer of a very incorrect risk model to say that employee data and employee candidate data is not a critical element that you should be raising your game and protecting as if it was the critical asset that it really is.

**David Greely** (07m 09s):
It's such an important point because when you bring up this topic of data hoarding and retention, you can imagine anyone goes out, they get a job, their employer, potential employer says, oh, well we need to do a background check on you, so give me your social security number. I gave got your name, I have got your address. Give me where you have been living for the past so many years, you are giving all this vital identity information that you really don't have much of a choice, right, like you need the job. It's a very imbalanced power situation and you don't have an expectation that all that data is gonna be given to a third party to keep. So how did we get there? Is it just not paying close attention?

**Michelle Finneran Dennedy** (07m 53s):
I am beginning to be a very broken record on vinyl. We need a federal law in the United States, this type of behavior in Europe, it's shocking to them. This has been covered by the 95 directive, recovered again when we revamped GDPR to try to make our privacy rules more efficient over there. An employee in the European theater, it's very difficult to show that that person had independence to actually consent because of the power disparity. You need that job. The only way you are going to get that job is sort of like a corporate gun to your head saying give us all your data. Well even if you have to have that trade off and there are security concerns, you want to make sure that you are getting the right people and vetting them appropriately. I understand the need on one side, but understanding the proportionality. So if I give you my social security number, am I giving you an ID credential?

**Michelle Finneran Dennedy** (08m 51s):
Not legally talk to the Social Security Administration. That is not an identifier. If you still have your old fashioned old timey social security card, it says specifically, this is not an ID. We treat our social security credential as if it is an identifier. So we expect to hand it

over to all of these places. By doing so, we have proliferated to a vitiate, its true credentialing power, and B, it becomes weaponized against us. So we need a federal law here to make sure that every employee has a consistent experience. Data centers are not segmenting state by state. We need to understand the value of the currency that we are handing over. We need to have a conversation about identity that goes beyond a credential that has been used and reused for in some of our cases over half a century and then we need to figure out how do we make sure that data has an end of life where appropriate?

**David Greely** (09m 54s):
I want to talk about the value of that currency as you put it with you because from our earlier conversations on the podcast, one of my big takeaways has been that we all need to understand that our data is a highly valued commodity with an entire industry around it that most of us are not even aware of and much like people learned about physical supply chains over the course of the COVID-19 pandemic, people now need to learn about data supply chains. So how do we get started thinking about this data industry and the data supply chains that support it?

**Michelle Finneran Dennedy** (10m 30s):
It's really important to, I think, start with the foundations. Let's go back to the mortgage crisis of 2008. Why was anyone able to resell a mortgage that was given out to a person with very little credentialing, if any. We had people who had no employment or very low employment, able to take out a lot of money with absolutely no backing whatsoever. Well, we were able to do that because we were able to bundle these things into packages and then resell those packages. You never would have said, oh look, it's a 18-year-old kid with two months of bartending behind him. Of course we will give him a home loan. You never would do that. So part of the reason with privacy to kind of like move into that analogy is the companies that are selling and reselling your information don't necessarily care about you the individual. So for the longest time, particularly in ad tech where we are making money by displaying things quote unquote for free, by sucking information about the use and the viewing of those ads, the use of those services, the companies were able to say, I don't care about Michelle Deity.

**Michelle Finneran Dennedy** (11m 44s):
I'm gonna call her Michelle X, we'll call that anonymized. We will put her in a bundle with all the Michelle X like creatures and we will start to auction off that attention to the highest bidder and over time we have seen regulations sort of try to catch up with that, but understanding that we as a group of people are very important to the world economy in the digital world buying and reselling. But we are also really important to understanding how we are a part, a fundamental part of how the sausage is actually being made. We are not just viewing ads. So what we are doing to try to understand how we interact, particularly with software, but it all trickles all the way back. The software is running somewhere. In reality, our quote unquote cloud services are all attached to actual servers and computers and databases. So at software, it's hardware, it's HVAC, it's energy.

**Michelle Finneran Dennedy** (12m 47s):
How are we having all of this data flow and how is it equally flowing? It's easy in that complexity and that expense to forget each individual element. So we are all sort of the blood flow and that's why I say data is not oil. Data is a currency because it's contextual. If I only have Michelle X and there's only five of us in the world, that's an important thing for people to spot and that's an important thing to serve. If there is a very generic sort of bell curve, amount of ish behavior, where do people drive on the freeway? We can get further, further back in the data center and shed some of those identifying elements. But that takes work to do. So understanding what is the output that we want, how deeply do we have to understand the data subject observe and then understanding the supply chain that makes elements of data very valuable or not is really a very large mind shift for a lot of folks who were brought up in the era of storage is cheap, it's only getting cheaper.

**Michelle Finneran Dennedy** (13m 53s):
Compute is cheap, it's only getting cheaper every 18 months. We double capacity, we half the price. That's how a lot of our senior leadership was really trained on data and IT services. The reality now is we have the capability quantitatively and qualitatively to make a lot of different choices and understand how do we actually make this currency as valuable as we can while simultaneously decreasing the risks that the legacy kind of sloppy or hoarding behavior compute has sort of wrought upon us and so we go back to the beginning, this data breach of this very large broker is a perfect example of this. Just a buildup over time of extraneous data that they never should have had. Lack of grooming, lack of curation, really diminishing the value of those data sets to the fiduciary, the owner of that brokerage while increasing the value to people who want to do harm with it, grab it, auction it off to people who want to commit identity theft, who people want to change identities as human beings. People want more access in spearfishing campaigns, et cetera.

**David Greely** (15m 07s):
I would love to get a little deeper into the supply and demand of it all with you. As you said, the cost of hoarding from a data storage perspective has only gotten cheaper. So there was no real cost of just amassing these huge data sets. But also it seems like in the beginning, as you said, a lot of this data collection was geared towards let's make our advertising more targeted. So we just kind of want to understand these groups so we can target at these groups. But it seems like even the targeting has gotten much more personal. I am sure I am not the only person who's experienced, you go onto a website to buy something, airline ticket, whatever it is, and all of a sudden like you get one price when you are logged in as yourself, somebody else, you know who you might be coordinating with, they log on as themself, they get a different price. And so it's become much more individual level than seem to have been 10 certainly 20 years ago. So I am curious if you look at the data markets now, like who are the buyers and sellers of data and what's the structure of intermediaries that connect them, are there lots of companies like national public data out there?

**Michelle Finneran Dennedy** (16m 15s):
There are thousands and thousands of these data brokers out there and I think we'll only find rather than them going away because we've had this massive breach, what we are going to gonna hear increasingly because of the sort of parallel phenomenon of AI and ML we are going to hear more of these data sets being required to train these algorithms to, as you say Dave, be more and more quote unquote personalized. I think that word has outstripped itself. It's not very personal. They are being very targeted in about the coldest of ways possible to figure out exactly how much they can juice out of you. What's your margin cost for your attention, what kind of price elasticity do you have when it comes to purchasing things? I think the airlines are a perfect example. I don't want to pick on them but I am going to pick on them. When we book a trip now I literally line up my family and we all check the same itinerary on different machines and we pick the best price because it wildly different.

**Michelle Finneran Dennedy** (17m 15s):
On the last trip I took, I was quoted $1,500 for a ticket across the country. My daughter was quoted $700. So is some of that because they have only one bargain price ticket per day, maybe I have a lot more status than she does. You would think that that would give me a preferential price. In fact it doesn't because I have a lot more elasticity than she has. So I think that we are going to see more of this. I know that we have thousands and thousands and I don't even know the number of brokers and I think they are also going through a phase of consolidation just like every other large business because you see things like these massive losses. So the smaller data brokers should be small and specialized. So there should be one specifically on certain types of healthcare and diseases to highly curate but the commercial imperative here is all of the protection, all of all liability and the capabilities of actually exploiting this data are becoming more expensive and more complex. So you do see them consolidating into these very large brokers.

**David Greely** (18m 17s):
And how does data like the social security numbers get into the supply chain? We talked a little bit about how like an employee check could be one way. How does the information get in? I guess how is it sourced? Is it legally but perhaps not ethically are we like fencing stolen goods here? Like what's going on?

**Michelle Finneran Dennedy** (18m 36s):
I think even where it's legal, I would say that given the state of cacophony and data privacy and protection law, you are not in compliance If you find a social security number, first of all its purpose is to record your income so that you get social insurance from the US government. That's it. That's the only reason that should be ever used anywhere. But we all know that's not true. It is probably your most important. In fact, on my college ID from way back in the day, it has my social security number printed right on the ID right out in public. Every credit card form you have ever filled out, we are addicted to instant credit In the US addicted, if we just stopped getting instant approval credit cards, we would cut down an identity theft. So the data's coming in through filling out paper forms that are not guarded.

**Michelle Finneran Dennedy** (19m 30s):
The data's coming through sloppy startups that the VCs are telling companies not to engage in security and privacy until they quote unquote get bigger or until they get bought. So you have got all of these little companies innocently trying their best. They don't have a credit card information program, but they are collecting things as sensitive and as much of a fulcrum as a social security number. I will tell you my own story, I think, I don't know if I have shared this on this podcast or not. I was advising a company on their advisory board called AllClear ID, fantastic company, Bo Holland, CEO there and at the time he was selling a commercial product saying think about LifeLock was one of their competitors to clean up after these massive data breaches and what they discovered is statistically anywhere

from 11 to 15% of the social security numbers that sought the free credit monitoring after a breach were children and very young children.

**Michelle Finneran Dennedy** (20m 32s):
And so he developed this thesis and then chased it down and found out if a child is not getting a college loan, getting a job, getting a car, getting a phone, they are not using that credential for a long time. Thieves love an open unlocked door. So fast forward, I tried out his service, I put in my child's number, I know his security was top-notch and probably the best day in the life of any startup founder Bo called me up, I will never forget it, I was skiing and he said, Michelle, I have some bad news that your daughter who is 8 has the worst credit score possible. Her number has been in use since 11 years before her birth. I was given a financial birth defect by the Social Security Administration and it was currently being used to traffic people over the border. It's those kinds of credentials from children are used to for pedophiles to get off of registries so that they can move around freely.

**Michelle Finneran Dennedy** (21m 33s):
They're used to get gun licenses for people who should not be getting weapons. So not only is that data very attractive, it's very attractive to exactly the type of person you want, nowhere near your child's credential and it's happening in urban situations right now when economic times are tough, there's a huge incidence of parents who have blown their credit taking their children's identities and using that credential to get more credit for themselves. The second thing Bo said to me was don't worry, we are going to steal it back and he did, but I was a chief privacy officer at the time. I was working with the head of a company highly motivated to fix this problem and it still took us about two years to clean up the mess. So every normal kind of Tom, Dick and Harry out there, what chance have you got? So there are these companies, you know, all clear ID still exists. So there is companies that will help you clean up the mess. But to your initial question, this data is being so freely used and freely given in the name of identity that we have gotten into a place where the supply chain for the bad guys is next to zero to get your hands on some of this stuff.

**David Greely** (22m 52s):
I remember very well when I was in college, my student ID number was my social security number too and you would walk down the hallway outside the professor's office to see grades posted and there was just a list of social security numbers with grades. So it's so disturbing to hear the uses it can get put to and how difficult it is for people to reclaim these identifiers once they have been taken that way. Because yeah, I was thinking for myself, I wouldn't even know where to begin. I am sure I would be calling you and people who don't have that access there is nothing if it takes two years with the most informed people in the world who have the best connections and know-how a typical person can't do anything, which makes you turn to what sort of regulation we need and what sort of regulation, if any, exists over these intermediaries at this point?

**Michelle Finneran Dennedy** (23m 43s):
The data brokers, the real upscale data brokers, they actually do have quite a few rules and regulations. So they are some of the more highly regulated and organized entities. I have to say there is certain ones that are great. In California in particular, they were reserve the lead state passage of privacy laws. You have to register with the state, you have to allegedly have privacy by design and I will say allegedly the legislation has been in effect for a couple years now and enforced, I don't know how big the backlog is. I can only imagine what it's like to be that regulator, but it's only a state. You are never going to have the gun power that you need to go after all of the brokers. So the cat and mouse of regulate something like do not track taking the time for each consumer to actually look when that little pop-up window comes and says accept cookies and not batting it away and actually going through the pain in the neck, gooey.

**Michelle Finneran Dennedy** (24m 40s):
That should be illegal in my mind. You heard it here first. Should be easy, should be yes or no and that should be it. You shouldn't have to go to multiple screens. But that's where we are and I think where change happens is instead of looking to the consumer to sort of bat a thicket of mosquitoes away and then pray they don't have malaria. Meanwhile there is a cesspool over here of water that's sitting there. These giant data sources, giant databases, training sets that are being freely traded. That's where the malaria is coming from. So getting into supply chain and thinking about privacy by design and privacy engineering for execution. The laws that are starting to include that requirement, and that does include Brazil, that does include the European theater, that does include Asia, that does include Canada. We're sort of the malaria pit here in the US. We have sectoral information segments that talk about doing secure processing of data, but really getting into the guts of having somebody who is a strategist at the top of the heap, your data strategy, someone who understands how the interface of law and technology meet like little gears for privacy engineering to become executed and really critically and this latest breach really shows your board has to have some accountability. They have it over fraud, but this is

the Enron period for data. Why in the world does this board have no idea about the weight and the import and the impact of the data supply chain? I think it's shocking and I think it's time for some accountability at the very top.

**David Greely** (26m 26s):
And that brings me to accountability. Some of these privacy by design approaches. I am trying to think of like what sort of regulations should exist over these intermediaries to protect privacy and personal data and I get that we want flexibility and we want people to be able to make choices. On the other hand, we are all aware of like the bazillion page privacy agreement that we all click yes and bat away. Like there is just this cognitive overload that we put on people to have to become experts in these very nuancey subjects just to access a website. So is there a role for just kind of putting a baseline of privacy in place and what sort of regulation would do that for us?

**Michelle Finneran Dennedy** (27m 15s):
I think that's right. I live in Silicon Valley, I have spent my entire career out here. After I was done being a New York junkyard dog litigator, I came out here to Silicon Valley to get even more on wash. We often cite the myth that regulation stops innovation. It's not true. You are an economist, Dave, you are the data guy. If you look at what happens when we regulate industries, we actually see a ton of innovation happen. So when we try to say specifically use exactly this form of encryption or use this strategy for anonymization, we will lose because the market moves too quickly when we instead say you must have an understanding of the data flow and that doesn't mean just what's going on from the application interface to application interface. That's where a lot of these quote unquote automagic privacy tools are. They are sniffing APIs and going, look, I can find, no you cannot.

**Michelle Finneran Dennedy** (28m 15s):
You need an architectural understanding end-to-end. What is your data appetite? What is your data output? How is this making you money? How is this causing you risk? Every company can know this, a tiny company can know this and then you get into what is your architecture for protection? If you are a data broker, I expect you to understand every single vendor down to the Rowan column of the type of data that they are allowed to have access to and how you plan to prevent over access. I expect you to have an end of life plan because that's who you are. It's like going into a neurosurgeon and saying, I expect you to know exactly, you know where everything is inside the login and how we are going to deal with things here. So I think by having a law that says we are going to start by you telling us what is your data strategy?

**Michelle Finneran Dennedy** (29m 07s):
Do you have an architecture? Do you have someone who's accountable at the top? It starts to be something that is manageable and actually invites innovation just as we did when we had the breach laws coming out in California. That law requiring you to simply just tell people when you lost their data so they could at least have a chance to chase it, that has invited over a trillion dollars of investment in the security field in the last 25 years. So it doesn't stop innovation. So I do think we need something that's broad enough to allow accountability, but also broad enough to continue to invite that innovation that will help us protect for the different types of businesses that have to flow.

**David Greely** (29m 54s):
Clearly on the podcast here, we are advocates of market-based solutions, but to have well-functioning markets, you need to have well-defined property rights. And we really need to get to a point where we have established that the individual is the owner of their own personal information in this market and I know you are doing a lot of thinking on data supply chains and markets. I just wanted to ask you, where do we need to go from here and thinking about data supply chains and markets and how to make them smarter?

**Michelle Finneran Dennedy** (30m 23s):
I am a market-based solutions person as well. I think if you overregulate or if you put a zealot in front of something and you say, I need to have a standard that simply doesn't exist in the industrial world today, you could be aspirational. But if you start doing that, all you get is non-compliance and chicanery. So only 10 companies will be in compliance and everyone else is messing around. The market has to speak. The way that the market speaks is starting to put, if not monetary, direct correlates, I will say on the market, you have to start to at least do some sort of a correlated value model. So for example, I had a situation where we had a data center trying to anonymize as much as possible in my past life at Big Corp selling globally, over 51% of our revenue was coming from outside of the US.

**Michelle Finneran Dennedy** (31m 18s):
You have to be mindful of countries that actually have regulation around ephemeral data assets. We were getting in our data coming back from our sales team pushback and contracts that were not being executed because of quote unquote privacy. So I said, okay, I am curious let's gather how much of this is happening and we found that it was over a million dollars in this one particular product per country per quarter. That's a lot of money, not real money when you are talking about, you know, tens of billion dollar company, but a lot of money and a lot of money to individual sales guys. So this is important. Now I have got an owner that cares what's going on in the marketplace, my sales guy not closing deals. So I follow that up the chain. What does that mean when we have a privacy problem? Well, they want unlimited liability for any data harms.

**Michelle Finneran Dennedy** (32m 08s):
Ah, I can fix that supply chain within my legal agreements and understanding how do I now control that risk? Well, sometimes it's just clarity of architecture. We don't really know where data is flowing. If it's flowing outside of a regulated jurisdiction, well I can do that too. I am an engineering shop, I sell software, I can be transparent about what we do. So we did that. So when you start to unlock the elements of why is your supply chain not flowing, or how much time and effort are you taking to hide that, you have a bevy of 2 billion social security numbers. Someone had to actively hide that information. That's a flag for me going, why are we wasting all this time hiding it when we can simply delete it? Once we did those pieces and I built a model, I then tracked not with my engineers who were building new products, not with my finance guys, I tracked with the contract negotiators.

**Michelle Finneran Dennedy** (33m 08s):
How can we track how quickly we are actually processing? I have got a customer that says, yes, I have got a product that's data saturated. How quickly can we get these numbers together? When we started tracking the time saved, getting deals done, the time to revenue and collection, the complaints happening in your service sector and then we figured on the follow on, it wasn't a million dollars per country, it was 10 every quarter because they were then buying more things from us. So I had a direct line of causative increase and then I had a correlated impact on poll. And then I looked at the number of people who are going to our club, the like fancy sales party where no HR person ever wants to be. 75% of them had changed their book and their presentation to talk about our data strategy even though they're selling a book of hardware.

**Michelle Finneran Dennedy** (34m 07s):
So that's the kind of technique as an example of in that technical sales context, I am not chasing down the CIO, I am not chasing down the security people. I am not going to all the usual suspects. I am looking at the flow and what does it mean to this entity and what does it mean to our customers who need to be satisfied? And that's the kind of motion I would like to see of you have to have, not just awareness, but you have to have organizational KPIs. You have to understand your inputs and outputs. It sounds a lot like a market.

**David Greely** (34m 43s):
Well, thanks for making us all a lot smarter about this market. I imagine this will be the first of many conversations on this important topic. Before I let you go, this is our summer playlist series and it's become a tradition to ask each of our guests what's on their personal beach reading list this summer. I wanted to ask you, what are you reading this summer, Michelle?

**Michelle Finneran Dennedy** (35m 05s):
All right, I have two. So one is an oldie but a goodie. I know it's summer, so of course you are on the beach. What are you going read, well, you are gonna read Infonomics. So I love Hubbard's work on metrics, how to measure anything and I love Doug Laney's Infonomics. This is now an older book, but it's about monetizing information as an asset. This is an old book. People who know, know how to monetize the data asset and not just as a liability and then the other one was, I can't find where the, who the author is, but it's called Who Killed Jane Stanford. So the founder of Stanford University, she's a, she was a wildly wacky kind of a chick. It's a historical novel, but it's written as in sort of a novel be treaty kind of format. So I am gonna find out who killed Jane Stanford and I will let you know who it is.

**David Greely** (35m 55s):
Thanks again to Michelle Dennedy, CEO of PrivacyCode. We hope you enjoyed the episode. We will be back next week with another episode of our Summer Playlist 2024. We hope you will join us.

**Announcer** (36m 09s):
This episode was brought to you in part by Abaxx Exchange, where trading in centrally cleared, physically deliverable LNG and Carbon futures contracts is now underway. Ready for smarter markets. Contact us at onboarding@abaxx.exchange.
That concludes this week's episode of SmarterMarkets by Abaxx. For episode transcripts and additional episode information, including research, editorial and video content, please visit smartermarkets.media. Please help more people discover the podcast by leaving a review on Apple Podcast, Spotify, YouTube, or your favorite podcast platform. SmarterMarkets is presented for informational and entertainment purposes only. The information presented on SmarterMarkets should not be construed as investment advice. Always consult a licensed investment professional before making investment decisions. The views and opinions expressed on SmarterMarkets are those of the participants and do not necessarily reflect those of the show's hosts or producer. SmarterMarkets, its hosts, guests, employees, and producer, Abaxx Technologies, shall not be held liable for losses resulting from investment decisions based on informational viewpoints presented on SmarterMarkets. Thank you for listening and please join us again next week.