SMARTER MARKETS

PODCAST TRANSCRIPT

SM158 | 1.20.2024
Setting Course | Episode 3
Michelle Finneran Dennedy, CEO, PrivacyCode.AI

We continue Setting Course this week with Michelle Finneran Dennedy, CEO of PrivacyCode.AI. SmarterMarkets™ host David Greely welcomes Michelle back into the studio to discuss privacy in the age of artificial intelligence.

Michelle Dennedy (00s):
I sort of look at data as being radioactive. So if you have the gift of having some insight that is about this human being carbon form that is me, then you now own a radioactive plant. So you have the obligation and the fiduciary obligation and the criminal obligation if you mess it up. So if you have a business that has customers or employees, you have the obligation, just like you do with money, to not commit fraud with it. You have to take care of it. You have to absolutely treat it as if it is the valuable thing that it is and make sure that you're doing all these things to take care of it.

Announcer (36s):
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, bringing you better benchmarks, better technology, and better tools for risk management.

David Greely (01m 16s):
Welcome back to Setting Course on SmarterMarkets. I'm Dave Greely, Chief Economist at Abaxx Technologies. Our guest today is Michelle Dennedy, CEO of PrivacyCode. We'll be discussing privacy in the age of artificial intelligence. Hello, Michelle. Welcome back to SmarterMarkets.

Michelle Dennedy (01m 36s):
Thank you so much.

David Greely (01m 38s):
I always look forward to having you here, and especially now, I'm really happy to have the opportunity to talk with you about the big issues in privacy and technology. Correct me if I'm wrong, but I can't imagine a bigger issue than those currently being raised by the mainstreaming of artificial intelligence, AI, the LLMs and Chat GPT and I couldn't hope for a better guest to orient us to this new reality and maybe I should start there. When it comes to changing how we need to think about our digital privacy, exactly. How big a deal is Ai and should that be our main focus right now?

Michelle Dennedy (02m 16s):
I think, I mean, I proudly and happily wear my, my Crown as Queen of the Geeks here, Dave I think. AI, I mean, and, and I, and I tip my crown to all of the true geeks out there to define, are we really in an age of true AI, artificial intelligence there's a huge debate. Are we talking about just LLMs, no, we're talking about a broad category of not just large language models, artificial intelligence, distributed compute. We're talking about a large class of data processing, distributed compute models, all sorts of geeky stuff. But I think the most important and exciting thing is that the mainstream markets, 12 year olds, are cheating on their home works using generative models. Hairdressing salons are thinking about using artificial intelligence to generate forms so that they can accelerate their businesses more and more. We're talking about using data to hopefully do the boring stuff and frighteningly, we're starting to substitute some of this AI to substitute fact checking and so there's upsides, there's broad sides, and it's happening in the streets and I think that's where we really need to start hauling out the conversations of the good, bad and the ugly in AI. So I think this is absolutely the time to be having these conversations and looking at this as an element of risk both up and downside risk.

David Greely (03m 48s):
Well, I'd love to get into the good, the bad, and the ugly of it with you. Maybe I'll start, I don't know if this will be a good, bad or ugly, but we'll, we'll start here and see where we go. I think many of us have unfortunately become accustomed to living within an attention economy, a surveillance economy in recent decades and I'm curious, does AI, as it exists today, change the economics and the business model of that surveillance economy?

Michelle Dennedy (04m 14s):
I think it does, and I think so. I'll be selfish for a minute here, and sort of self-congratulatory. So almost 10 years ago, January 28th, in 2014, we published a book called The Privacy Engineers Manifesto as myself, my father, and my co-author, Jonathan Fox and in that book, we were talking about something called IOT or the Internet of Things and the Internet of Things is a synergy of sensors. So the Internet of Things was anything that gathered intelligence, right. So recording of voice, recording of video, recording of data everywhere and it was surrounding us and it was surveilling us and it was gathering things. So in talking about the internet of things 10 years ago, what we were talking about was where we are today. Why were we gathering all that data to have insights, to do analytics, to gather intelligence, to make decisions. And so we haven't come here by surprise.

Michelle Dennedy (05m 13s):
So it has been the case in the past that we've been making large decisions. We've been making decisions about whether to bring an umbrella to work based on the surveillance of our weather. We've been talking about commodities on this very podcast for a long time based on the surveillance of marketplaces and so the surveillance of our activities in our everyday lives has gotten more and more intense and more and more intimate the surveillance of our homes, of how high we turn our temperatures, and more and more intense and intimate on our phones, our everyday activities, every stroke that you take, every, every word and character that you type and so the intensity and the intimacy and the accuracy of this surveillance starts to intensify how much every company can surveil every government, and now peer-to-peer, how much work that we can do and so that's where we've come to where we are today.

Michelle Dennedy (06m 05s):
What are these work streams, what are the data sets that can be collected, what are these sort of meta models of insights and outputs and decisions that can be made, what are the assumptions that can be made and what are these sort of dossiers that can be assumed about you and you and me and I think, you know, we can all sort of start to build the story in our, our minds abou1t how dark we can quickly go now that all these sensors and all of this data can be collected and, and compiled all around the world about us.

David Greely (06m 37s):
And that's such an important and worrisome point because I know for myself, I often think of online privacy as what am I actively putting out through, I go on the internet, I go to Amazon, I'm buying things, I'm searching things on Google like, okay, I'm intentionally leaving a, a paper trail, as it were, a digital trail out there, but I don't think about am I being monitored in my home you know, like, is my, is my refrigerator reporting on me. Sometimes you think about, oh, is Alexa, Siri listening in, but I think it, there's much more passive revelation of our, our activity than there was in the past. Does AI change how that's used or does it just make it cheaper for people to access all that information that's already being collected?

Michelle Dennedy (07m 20s):
I think it's both. It's never been easier and cheaper and, and more democratized. So in the past, it was hard for the average Joe to gather information about you in particular. It was kind of like it was easy for the government in the 1970s was the sort of the first laws, particularly in the us there was a lot of laws in the, the, the first book that I saw was written, it was called The Right to Privacy in in 1974 and it was about government gathering information about what citizens were doing because there were large databases being created. That was the first kind of, it had a cartoon on the cover, and I saw it in my dad's bookshelf and I said, what does this right to privacy and this is when Westin was writing in, in Princeton about privacy rights. I was a little kid and I saw, Ooh, a cartoon that's fun, tells you what kind of a geek I was and what kind of a geeky upbringing I had.

Michelle Dennedy (08m 13s):
But that's that we really talked about governments and they had that kind of compute, and there was debate about citizens and governments and what was that relationship and it was really about surveillance you know, what could the cop on the street know about you and, and what were our relationship to citizens. Now you can buy data or you can borrow data, and we can sell and really trade data from data brokers. So I think that's where we're starting to see, not just starting, we're in the thick of even regulation we're seeing out of the European Union now that we're, we're seeing the finishing touches on the EU AI regulatory acts, and they're really

looking at it through the lens of product liability. So rather than just saying, this is just a nation state versus nation state, or a transfer as a transcontinental issue of government to government, they're looking at this as a company to company issue of product liability.

Michelle Dennedy (09m 10s):
If you're gathering algorithms of how you're going to look at the commodity of batches of data, and you're gonna make decisions, almost like credit reporting, we're gonna start looking at those algorithms. How are you determining what decisions you're making about Dave, who is Dave Greely, are you deciding that he is a bad guy? Are you deciding that you should charge him more because he's a rich guy? I mean, he has this podcast about smarter markets. He must be a rich guy. You should probably charge him more. Michelle, she's probably a poor guy. She's just a guest. So deciding who I am and what I am and what I get, are we discriminating? Are you a man? Are you a woman? Does that determine what we get? Should society have a say? So all of these sort of judgment calls and decision makings, and are we being discriminatory?

Michelle Dennedy (10m 02s):
And who gets to say what to who. These judgment calls, these batch processing, these predetermined roles that we're deciding are all determinative things that are becoming algorithmic. And so these, these judgments and these calls and the transparency that we're assigning to these predetermined mathematical decisions that we're making are all going into the calculus of how we're looking at artificial intelligence. And that's why this matters. So where we, we used to say in our silly sort of way of like, oh, it doesn't matter. I've got nothing to hide. Privacy doesn't matter. We thought we were just an individual person sort of skipping through the digital landscape alone. Now we start to see where the momentum starts to build, where as a society of billions of different data transactions, we start to build up and we start to make all sorts of additive decisions and multiplying decisions and logarithmic decisions together. We start to see where this can cause tremendous cultural harm and societal harms. So that's where we're trying to get in front of this with regulatory action, but also on the side of commerce and on the side of individuals. So we have a lot to say as customers, as companies, as innovators in the space.

David Greely (11m 26s):
And I want to come back to your point about the algorithms, because it's really fascinating. We've had other guests talk about, if you want to get your hands around this, you got to get your hands around the algorithms. It sounds like in Europe they are trying it from a product liability standpoint. Others have advocated for transparency. You know, in some sense, do the algorithms have more privacy protections than individuals at this point you know, of falling under some sort of, I guess, intellectual property of the companies that own them?

Michelle Dennedy (11m 56s):
I think in many ways they do. I think it's very interesting, and I think that's an interesting way to look at it is an individual has a very hard time of distinguishing themselves or are finding their way. So we have this notion particularly in countries that have an omnibus privacy law. So we do not have, amazingly enough in the United States, we still do not have a federal privacy law. But even in, in economic areas like the European Union where they have the general data protection law, GDPR, you have the right to correct, you have the right to delete. Supposedly, it's incredibly difficult for an individual person to functionally go through a data center group entity and, and functionally go through and, and know that your data points have been cleansed and, and deleted because you're, you're part of a group and part of it depos the quality of the rest of the data set because data quality is part of a group, because we're part of a society.

Michelle Dennedy (13m 07s):
So deleting data is not the answer per se. I've always sort of rebelled at the notion of data deletion or, or sort of, do not do this to me as an individual is the answer. Because what it does is it actually discriminates against the other dataset. So it can actually harm other people's rights if you just say, oh, I'm just going to delete my data. You're, you're probably doing more harm than good. That's an overstatement oversimplification of the problem. But what it says is exactly as you say, Dave, is it could be that we're overprotecting algorithms unless we put a full balance of algorithmic intensity. So you look at the scrutiny of the algorithm itself, you have to look at the accountability of the system overall, look at the impact, have the ability to correct and have the sort of fungibility and flexibility built into the system in advance so that you know that there's corrective measures that can be taken. There's flexibility so that you can make corrections, and that you don't have just an omnibus zero or one so that you're either throwing out all the data or you're keeping all the data. There's either one algorithm or zero algorithms, or you're doing a series of sort of decision trees so that you can have corrective measures made along the way.

David Greely (14m 28s):
I'm intrigued by this idea that, that I kind of hear in what you're saying of almost data as a product, data as something that's being sold in batches. You know, it's almost like there's the commoditization of data and there's a marketplace for it. I think often I think of it as, oh, the company's collected and the companies use it, not that it's being packaged and sold and marketed. B2B, I suppose, what is that data marketplace like?

Michelle Dennedy (14m 57s):
Yeah, so I mean, there's, there are people that are far more skilled at this than I am, and, and you'll find them in the ad tech space. So you can find folks who know down to the penny how much an impression is worth. For example, I think some of that skillset can be applied here for algorithmic building and buying and selling. Now, it can be excoriated in a certain way, you know, are we, are we buying and selling data about people? But I think on the upside, understanding actually how we package and, and control and modulate and actually venerate the value of building and valuing data is not a terrible thing. We value quality food. I value an experience at the French Laundry, and sometimes I value a meal at McDonald's. And so the quality and the experience might be a different sort of experience, but I know what I'm getting when I'm going there.

Michelle Dennedy (16m 01s):
And so it, it may be that those kinds of experience of a data broker, it doesn't mean that they have to go away, but understanding transparently what they mean might be a very important thing. And so having the modulation and, and the skillset of understanding that data brokers exist and they may not be these giant sort of oligopolies that they are today, I think every digital entity will have to have some of that skillset. And just like you have a CFO that deals with your currencies and they're starting to be pushed on by the digital currencies, you're going to have a data officer that should be invited into the boardroom and they should be looking across your algorithmic landscape with that same level of sort of power and budget power. And they should be looking across, and this is what my business does at PrivacyCode.

Michelle Dennedy (16m 55s):
You're looking across the regulatory landscape. You're looking across the capability and the competency in the systems with that same eye to value and saying, what am I capable of doing with my data? I'm not looking at my data landscape like it is some sort of hoarder's den. I'm looking at it as I'm keeping what I need. I'm expunging what I do not because I'm the excess turns into risk. It doesn't turn into, like we used to be told in, in, in it that extra data or more data, like suddenly you're gonna get, if, if you have excess data, somehow a pony is gonna come out of it. No extra data is not like you're not gonna dig through pony poo and find a pony, you're gonna find cholera. So you got to get rid of that stuff. You got to start to look at your IOT data as something that might turn into a commodity. Only if you build it into a positive algorithm that you can build, show into something that is sort of going somewhere. If it's not, then you need to get rid of it and then prove that it is gone.

David Greely (17m 58s):
And when you think about what data is valuable in the context of what we can do with AI, is that changing the type of data that's valuable or is it just increasing the value of all types of data?

Michelle Dennedy (18m 13s):
I think it's a little bit of both. I think it's the cool thing is there, there are so many people that are really old school that have been talking about quality for so long and their voices have been kind of, it's kind of, yeah, yeah, yeah old school, but quality matters and so understanding that a really good customer, it's really sort of uncommon common sense. A good customer is a customer that is recurrent. A good customer pays their bills on time. A good customer wants good quality from you. They read your materials all the way through, you know, they sit in the front row there, there's aspects of the way that they behave and there's aspects of the way that they interact with you and, and that it's data to prove that that is data quality and there's algorithms to show that and so instead of looking at like peckish clicks on your website, and that's how we've like marked our marketing people are getting scored for like click, click, click, click, click, click, click.

Michelle Dennedy (19m 13s):
That hasn't really translated into dollars. And so now we're where we're kind of the death of the cookie is going away thanks to the, our European friends, we're starting to go back to the old fashioned, like marketers are getting scored on different things. We're starting to realize, aha, maybe the old fashioned customer means x good employee now that we're all remote and hybrid. Maybe having a task that your employee is supposed to complete at a certain date is different than is Billy sitting in his chair at X date and maybe we should

put a sensor in his chair. I've heard these proposals at work. Yeah and they've, you know, as a chief privacy officer, people have said, well, can we put sensors in in our employee's chairs and then give them five minutes to go to the bathroom and these are honest and earnest people not trying to be jerks and I'm like, no, no, not because it's a privacy violation, because it's stupid and sometimes you just have to like wake them up a little and they're like, oh yeah, that is kind of dumb, isn't it?

David Greely (20m 23s):
Dumb. Oh, it sounds awful and it's interesting it's like there is always new privacy issues being brought to the forefront. That's certainly one, you know, as your chair minding you.

Michelle Dennedy (20m 34s):
Super excited about it, oh, like, no, no, we're not doing that.

David Greely (20m 39s):
And I wanted to ask you about, you know some of the other new privacy issues that might be created by this AI technology that we have, you know, you read news stories and you hear about fights over unauthorized use of intellectual property, you know, basically, oh, you took my book and put it in your training dataset and now the AI's putting out writing that sounds an awful lot like what I wrote. So kind of like high tech plagiarism and concerns that AI can reveal in its responses, private information that may have been hidden within its trading data. If you train it on social media accounts, maybe it digs something up and reveals something that, that it shouldn't, what do you make of these issues and what are some of the other new privacy issues that you're seeing or imagining could be created in the future through the use of AI?

Michelle Dennedy (21m 30s):
Yeah, I'm so fascinated by things, you know, like the Getty case for images and you know, I mean, I think my, my book is an interesting case because it's open sourced through a common license. So you know, it is available. You can download it through a press.com or, or if you've got a Kindle or a Nook, but it is, you know, it is through a license, so it shouldn't, you shouldn't just publish it without giving it credit but if you, you know, in the earliest of chatGPT, you could get huge uncredited chunks of it and I thought, well, that's not cool. I'd like at least a citation to it. That's not cool. But it, you know, it isn't fair for, for full passages of, of people's work to be unsighted and it is dangerous for people to present things that are not fact, that are not factual, that are in fact fiction.

Michelle Dennedy (22m 22s):
And the other part of it is, is the other part of the dangerousness, particularly in these times and you should check out a, a short documentary by Gale Anne Hurd. She wrote The Terminator with James Cameron, and I had a wonderful chat with her, and she is very much in the advocacy side about AI because it's emotional, AI can be emotional and she said, what is your interest in AI. I'm a geek and I'm a former IP attorney litigator and she said Jim and I warned you about this in 1982 and I thought, who's Jim and I thought, well, I think of him as James Cameron. I don't know him as Jim, but that's when she put in the copyright treatment for the Terminator and I had never thought of the Terminator as being a warning about artificial intelligence, but Arnold Schwarzenegger was a desar gone wrong.

Michelle Dennedy (23m 16s):
It was a desar attack trying to erase Sarah Connor coming back and trying to erase a data element that was gonna be the mother of the man that was trying to ruin the machines and so someone was trying to erase a data element from the database, and I thought, wow, that's so fascinating. But she just published a documentary called the YouTube effect and so it's really talking about how people can be really radicalized by content and so with the advent of stuff that is not surrounded by context. So if something comes from the New York Times versus the Babylon B versus, you know, the Sun Times or the fifth page cutie or whatever, it just sounds and feels like facts. And so whether or not it's protected or someone's getting a license fee or some of the other handfuls of rights that surround what we know as intellectual property, so is someone, the author getting their due or not to the person who's consuming it, it lands differently emotionally as a fact.

Michelle Dennedy (24m 20s):
And so you don't get the same amount of context. You know, you're not getting that sort of Richard Attenborough factness you're not getting, you're not consuming it in the same sort of academic way. So I think that's, that's one factor and then the other piece of it is, I think the nature and curiosity and texture of inquiry changes a lot. And so facts become very slippery so that you don't have the same sort of selective way. The way that the beautiful thing about the way that the human brain works and the way that artificial intelligence

does not artificial intelligence is wonderful at collecting. Your brain is wonderful at forgetting. It's designed to forget. And it's, it's designed to only selectively process and we're getting better and better in compute at computing massive things and so that's where these two things are very, very divergent and we forget about that, so there's tons of issues on ownership rights, there's tons of issues on how will we actually control the societal issues. There is tons of issues on the impact and the harms and the discriminations and the privacy, and I mean privacy as the authorized processing according to moral, ethical, legal, and sustainable rights. But there's also an issue on how are we actually containing and controlling and managing systems and understanding where the edges are of these systems. So that was a massive mind mouthful. So wherever you are listening to this podcast.

David Greely (26m 03s):
No need to apologize. I don't know. I was trying to think of like the good sides and the bad sides of the technology. The bad takeaway on AI is it can feel like the guy we all hate to be next to in a meeting, right. Overconfident says things like, he knows they're true, even if they're not and takes credit for other people's work, it's like, how do we get.

Michelle Dennedy (26m 25s):
An edge on it like you just, it's so slippery that you're just like, he has a really nice English accent and a deep voice and it just sounds so good, but you can't really figure out where the wrong is. But you know it in your gut. Something's up.

David Greely (26m 39s):
Yep and I wanted to follow up with you on, on the first point you were making because I think it's really important in that it's not just about collecting data on us and then doing something with it right now with artificial intelligence. It's becoming very easy and inexpensive to create these bespoke experiences for us and I wanted to ask you about how do we think about the violation of our privacy required to create those experiences because you need to know a lot about us. Is this like simply the next step in the progression of cookies with targeted advertisements, online shopping suggestions, tailored Google searches, you know, or are we moving into a world where we're each getting our own personalized reality that may or may not overlap with the experience other humans around us are getting?

Michelle Dennedy (27m 30s):
I think there's a very big danger in that and I think there's a couple of things and I think my worry is and it's more for my girls than it is for people like you and because my girls are very good at curating their personas. Like, I am kind of like a splatt. I'm kind of who I am, for better or for worse. I'm a mess and I am who I am and it's kind of too late for me you know, I have sort of my inside voice and my outside voice, and it is what it is but I've been this way for a super long time. My girls have grown up as digital natives and they're good at being one thing on one platform and one thing on another platform and I see them now emerging as young adults.

Michelle Dennedy (28m 19s):
And it's very interesting because they're far more guarded than I am when they cross the streams and I've made a lot of embarrassing mistakes because I am who I am and I will say dumb things in meetings as at home, Michelle, but it is what it is and I wonder sometimes if that's gonna be the case, is that you'll have these little chunks of people, or if it will be the case where the other case is true and you will just be assumed to only be the, the kind of average of all of your best and worst selves and that's it and you can't transform, you know, like you're always that person that ran up on stage and slapped somebody because you're an idiot instead of, you know, being whoever that guy is at home and I don't know the answer to that, and I think it's kind of too bad because people are so complicated and you should have the right to become something totally different if you want to do that and I do think that people, there's a core of us that that is the same but if I look at myself over the years, I never ever could draw a linear line from where I was then to where I am now. It's such a jagged strange place that you know, if someone else had an algorithm and decided for me, I would still be, you know, living in the Midwest making multi-layer cash rolls.

David Greely (29m 48s):
That's really fascinating that it can kind of limit the ability to grow and change, I guess, if it's always just reinforcing who you currently are.

Michelle Dennedy (29m 57s):
Yeah and that, that's how we used to be, you know, there was a lot of assumptions about, you know, what I was supposed to be and the same.

David Greely (30m 05s):
Yeah. Back to the future like the whole generational aspect's really fascinating. Like you brought up earlier, you know, about the old things being new again. I remember, I think my, my parents' generation, my parents in particular were probably like the last people on the planet to get credit cards because they're like, why are we giving all this information and who's gonna use it and they could get access to it and suddenly I owe all this money. Or to like, anytime you'd sign on to a website, like, okay, who's getting this information like, they were on top of it and I was the younger person being like, oh, what are you worried about it's fine. You know, kind of like the, I guess it was privacy through obscurity, like who cares what you're doing? Nobody's gonna go to the bother to try to follow you around and probably my generation kind of lived with the internet that way, right? Like, oh, we're small fish, it doesn't really matter. But now it's so cheap Yeah. To find us and not find us statistically not like, oh, we're gonna look at a data set with a thousand people, kind of like you and slice and dice it, but you can kind of find that individual person and thinking about your daughter's generation, the next generation, like all of us, how does like the mainstreaming of AI require each of us to change our mindset about privacy?

Michelle Dennedy (31m 19s):
Yeah, I think and it's very interesting to me too because I think some of the, the privacy advocates, like real advocates define privacy as the right to control all of our information and I think, gosh, as a systems person, and I've always been on the systems side, you know, from Sun to Oracle to Intel to Cisco, I mean, these are the monoliths of control. You don't actually want that. You, you want the systems people to have to do some work here. It is a lot of work to control the quality of a system. I can't imagine a world, I mean I can barely get my taxes done. It sucks in the US that we have to do all the taxes given how much the government knows exactly how much money I don't have as a startup owner to actually have control over all the algorithmic decisions being made.

Michelle Dennedy (32m 15s):
So I think that to in the future, to be able to have some control is important to absolutely have the sort of look at data as being radioactive. So if you have the gift of having some insight that is about this human being carbon form that is me, then you now own a radioactive plant. So you have the obligation and the fiduciary obligation and the criminal obligation if you mess it up. So if you have a business that has customers or employees, you have the obligation, just like you do with money to not commit fraud with it. You have to take care of it. You have to absolutely treat it as if it is the valuable thing that it is and make sure that you're doing all these things to take care of it. Just, you know, like a hotel room, like you're not allowed to go in and rape the people that sleep in those beds.

Michelle Dennedy (33m 10s):
So you have to have the care and you have to spend the money and you have to invest in, in, you know, not poisoning the food. Don't rape, don't rape the people in the beds, and the people too have to lock the doors and shut and shut their shutters and do the basic stuff. So we have to dance together as a society. So people have to be more educated about what they're doing with their data. You have to have a certain, just like with your money, you have to be educated about what data is and how powerful it is. You have to just like, you know, I was taught as a young girl, you know, the power of reputation and even more so, you know, in, in younger days people were taught about the power of reputation. I think it's really instructive actually in, in the Asia countries that are an older society.

Michelle Dennedy (33m 53s):
They're a much older society than we are. The power of face of ancestral reputation is so much more powerful. They've had more time to understand the power of privacy. They don't have the word privacy. It's very interesting. They don't have the concept of privacy. They have the concept of face, they have the concept of reputation. It's much more powerful to have familial security and, and ancestral and I find that very, very interesting because I think that's where our society is sort of catching up. So as much as we sort of look down and cry, what's going on and I'm not venerating some of the, the dictatorial behaviors that go on, but when you look across long-term societies that sustain a cultural identity, you see that individuals look out for each other as a society. You look at individuals take responsibility for their own actions, and you look at cultural people that look as ethically across and, and take responsibility for looking out for each other's their data stories that they tell about each other.

David Greely (35m 02s):
And I always fear when talking about some of these issues that I get too negative on the technology, but I think in the case of privacy and risk, it's probably accurate to focus on the risks that they raise but ultimately, AI, LLMs chatGPT, what have you, or tools and tools can be used for good or for ill the good bad, the ugly, you know, usually it's some combination of all of them. I was curious, you know, when you look out in terms of privacy, are there ways that we can be using AI as a tool to better protect our privacy?

Michelle Dennedy (35m 38s):
Absolutely a 100%. I mean, our company, I mean, we're called privacy code do AI. I mean, before the whole chatGT popularity happened, we were called AI, we use an LLM to actually wade through documentation and, and we, we leap ahead. So we wade through pages and pages and pages of legalese to produce a prioritized task set and so we, we'll, we'll basically take what used to take months, even years of conference rooms, meetings and consultancies and prioritize what you need to do and for some people they're like, oh, but I still got to do the work. Yeah, you do, but I've just saved you a year. Like, sorry, that still, you still have stuff to do but that alone starts to get the work done and once we start getting into the systems, now that we've said, here's the system that you need to build, or here's where you need to get going or here's what you're gonna build for your privacy by design systems, then we can start to even go even further.

Michelle Dennedy (36m 41s):
So now we can apply more tools in the privacy enhancing technologies and use AI tools within the tools to start to do insights so that your systems are reading on systems to get to gain insights. Now I'm looking where the fault lines are coming because there's so much complexity within these systems that you need to build in systems to just like you're looking at with a commodity system, you can't do commodities trading without looking for faults. So just like when you're putting a collar, like if, if you're getting too much trading on a certain stock and, and now we can put the brakes on, you're gonna do the same thing. When you're starting to see an algorithm that's gone rogue or you're starting to like see biased trading or you're, or you take in or you're doing an m and a transaction and you see that there's zero permissioning on children's data, you're gonna put the brakes on that and you're gonna do some inquiry there. So putting brakes on things, letting things like go into a basket where you're gonna do inquiries, there's all sorts of ways I think that we can positively use some of the same exact tools that we're using to make money to do checks and balances, to do quality checks, to make sure that we're sort of, you know, we, we've got the tools, why not use them for good.

David Greely (38m 00s):
And when you know, are talking with other privacy professionals, that ability to use it for good the opportunities it creates to, to better protect privacy as well as the risks that it raises, is that shifting the conversation that's occurring among privacy professionals and corporations that need to be, that have a responsibility to protect privacy?

Michelle Dennedy (38m 24s):
It's a 50/50 shift. It's really interesting. It's some folks come to the table as a risk person because they are looking for risks and they're looking for downside risks and they're like, aha spotted one, and that's kind of their job. They're looking for that thing and they're like spotted one, spotted one, and they're moving on to spot the next risk and that's fine and that's kind of what they do and that's their jam. Other folks are looking proactively to be like, okay, found it now let's proactively partner and do something proactive and buy some new technology and get in, you know, get in and fix it and, and jam side to side and I'm more of that second kind of a person. So you kind of have to just keep eyes out and you know, remind yourself that there's, there's more than one type of mindset out there. So sometimes it's a CTO rather than a privacy person and sometimes, you know, people will surprise you. I mean, sometimes it's an auditor that's the most proactive and excited about innovation in, in this space. So there's a lot of innovation, you know, hey, any venture people, hey, we're raising our own, there's a lot of tools to be built in this space because as fast as we're building, that's as fast as we're building new gaps, right? So it's sort of a, it's, it's such an interesting and creative space out there.

David Greely (39m 47s):
It really is and I really appreciate you talking with us about it. Before I let you go though, I wanted to ask you one more question. You're both an entrepreneur and an innovator and you know, when you look out at the space now with the landscape being changed by the new tools that we have, where do you see the, the biggest room for innovation. What do we need to be doing differently in the future when it comes to privacy and this technology?

Michelle Dennedy (40m 14s):
Wow, it, I mean, it's amazing to me. This is such a blue ocean. So what do we need to be doing differently. We need to buy stuff. I mean, it sounds so basic, but we need to, we need more buyers. We need people to try stuff. We need people to buy stuff. We need to not look at this as insurance. This is the painkiller. The pain that you are killing here is if you think that you are going to wait for regulation to get in front of innovation that is going to get all your unstructured data to be the next chatGPT boom, to be the next thing that's gonna get all your unstructured data. That's, everyone's gonna try to do cost savings to get employees out. That's not gonna happen. We ran that experience with BPOs back in the audience.

Michelle Dennedy (41m 14s):
Not gonna happen, but you are going to get forms filled out for you with AI. You are gonna get more productivity on your calendars and you're gonna screw it up with AI. You are going to get more and more documents written that are gonna have to be proofread with AI. You are gonna get health forms screwed up with AI. So get your stuff together so that you can get your privacy stuff taken care of, get your stuff together so you can check for your intellectual property. Make sure that your lawyers are ready to roll because you're gonna have a lot of work to do from the class action bar because they are rocking and are rolling and it's global baby. So it's time to prepare for this stuff. So there's, there's tools to be bought, there's fights to be fought, there's lots and lots of policy work here and it's blue oceans. So get yourself a boat, start paddling.

David Greely (42m 18s):
Thanks again to Michelle Dennedy, CEO of PrivacyCode. We hope you enjoyed the episode. We'll be back next week with our next episode of Setting Course. We hope you'll join us.

Announcer (42m 30s):
This episode was brought to you in part by Abaxx Exchange. Market participants need the confidence and ability to secure funding for resource development, production, processing, refining, and transportation of commodities across the globe. With markets for LNG, battery metals, and emissions offsets at the core of the transition to sustainability, Abaxx Exchange is building solutions to manage risk in these rapidly changing global markets. Facilitating futures and options contracts designed to offer market participants clear price signals and hedging capabilities in those markets is essential to our sustainable energy transition. Abaxx Exchange: bringing you better benchmarks, better technology, and better tools for risk management.

Announcer (43m 19s):
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.